OCTOBER 2021

NORAD MODERNIZATION FORUM
INFORMATION DOMINANCE

The report was produced by a rapporteur from the North American and Arctic Defence and Security Network (NAADSN), a Department of National Defence MINDS Collaborative Network.

CONFERENCE OF DEFENCE ASSOCIATIONS INSTITUTE

INSTITUT DE LA CONFÉRENCE DES ASSOCIATIONS DE LA DÉFENSE

Introduction

The CDA Institute, in partnership with NDIA and NORAD/USNORTHCOM, hosted a virtual industry roundtable focused on the topic of achieving Information Dominance and the means with which NORAD and USNORTHCOM can achieve it in the digital age. The aim of this session was to allow experts from industry, academia, and government to break down silos and engage in direct conversations. More specifically, the goal of this event was to examine the architecture, infrastructure, data framework and policies needed for the integration of systems, as well as for deeper integration with allied partners.

This report, focused on Information Dominance, will outline the major points of consensus and contention reached by participants during the webinar, answers provided in the question-and-answer session, a synopsis of introductory remarks, updates on the Pathfinder Initiative, and a synopsis of the scene setter. This report was commissioned by the CDA Institute and is intended to read as an overview of the key points made by our invited experts.

NORAD Deputy Commander Lieutenant-General Alain Pelletier gave introductory remarks. An update on the Pathfinder Initiative at NORAD was given by Canadian team lead Colonel Robyn Hulan (OMM, CD, COO for N2X/Pathfinder). Colonel Matt Eberhart, Special Assistant to Commander of NORAD/USNORTHCOM, provided the scene setter. Gordon Venner (CDA Institute), Former Associate Deputy Minister of National Defence, Canadian Diplomat, and Ambassador, acted as Master of Ceremonies and moderated a panel discussion that included:

- Tom Karako, Senior Fellow, International Security Program, Director, Missile Defence Project, Center for Strategic and International Studies (CSIS)
- Julia Scouten, Senior Manager, Cyber Security Team, KPMG
- Chris Pogue, CEO, Thales Canada

The report was produced by a rapporteur from the North American and Arctic Defence and Security Network (NAADSN), a Department of National Defence MINDS Collaborative Network.

Executive Summary

North American continental defence is undergoing a transformational modernization amidst the digital age. Emerging technologies and emboldened adversaries are creating the environment necessary for NORAD and USNORTHCOM to achieve information dominance. The Commander needs more information from an updated sensor network that includes data from all domains. This will allow for a fuller understanding of possible threats from adversaries and create more time for decision-making, with informed and trusted data needed to broaden the possible choices and options to achieve Decision Superiority.

NORAD is responsible for the aerial defence of the continent and warns of maritime threats approaching North America. The binational command has evolved from deterring Soviet long-range bombers during the Cold War, to countering Violent-Extremist Organizations in the wake of 9/11, to addressing new threats associated with the reemergence of great power politics. This has created a new reliance on Information Dominance and cloud computing to protect the continent. These new modernization capabilities will ensure NORAD and USNORTHCOM can move "farther left of bang" (i.e., before there is an attack) by preemptively deterring and detecting threats in competition and crisis.

Experts from across industry, academia, and the command discussed a wide range of issues related to achieving Information Dominance. This included the Pathfinder Initiative, the military's ability to leverage and maximize commercial and private input, the possibility of working beyond traditional binational NORAD structure, and the challenge of keeping pace with evolving and emerging technologies with new actors in new domains. NORAD Modernization is a large-scale moving target, and decision-makers are scrambling to meet existing challenges and those yet to emerge. The allocation of resources amid these rapid advancements means that achieving Information Dominance is necessary to protect the homeland, as it is no longer a sanctuary.

All-Domain awareness should enable Information Dominance, which creates Decision Superiority, the ultimate objective for the Commander. For NORAD to Deter in Competition, Deescalate in Crisis and Deny and Defeat in Conflict, the binational command requires Global Integration, Domain Awareness, Information Dominance, and Decision Superiority. Ultimately, Information Dominance will allow NORAD and USNORTHCOM to meet three goals: 1) Improved decisions in competition, crisis, and conflict; 2) Proactive options to deter, deny, and if required, defeat 3) Global Integration across tactical, operational, and strategic levels.

Points of Consensus

- NORAD Modernization seeks to provide time in the Commander's decision space and Observe-Orient-Decide-Act (OODA) Loop. The only way to provide this time is to trust the data disseminated from the legacy sensor network and creation of new sensors (including space, over-the-horizon, or elevated). Data must have secure pathways, secure access, accuracy, and time-efficiency.

- Adversaries can exploit gaps (in capabilities) and seams (of command jurisdiction). The United States Unified Command Plan (UCP) creates areas of responsibility which can be problematic. The future of war fighting does not have geographic lines as adversaries are no longer restricted by traditional battle spaces.

- There are challenges between interfaces and seams in engineering designs that could allow for adversaries to impede the Commander's OODA Loop.

- The United States and Canada should assert sovereignty in the Arctic to keep a watchful eye over competitors. Investment in infrastructure, capabilities, and personnel is necessary to avoid a possible flashpoint of contention. Tools such as icebreakers, an upgraded sensor grids, development of cyber operators, and an evolved information architecture were mentioned.

- Information Dominance requires Global Integration. This means that allies of Canada and the United States need a coordinated allied effort to provide, ingest, and aggregate trusted data to achieve Information Dominance.

Points of Contention

- There was debate regarding whether NORAD should remain focused solely on air and maritime domains or seek to become a revised All-Domain binational command with a new overarching mandate.

- There was discussion about whether NORAD should adopt allies outside of the binational command framework, such as the Five Eyes intelligence sharing alliance.

The Case for NORAD Modernization

Gordon Venner (CDA Institute), Former Associate Deputy Minister of National Defence, Canadian Diplomat, and Ambassador, discussed mutual U.S.-Canada commitments in modernizing the North American Aerospace Defense Command (NORAD). Page 61 of 2017's S*trong, Secure, Engaged*, states that "Canada will work closely with the United States to ensure NORAD is fully prepared to confront rapidly evolving threats, including by exploring new roles for the command, taking into account the full range of threats." Recent joint readouts from President Biden and Prime Minister Trudeau have discussed important defence and security issues including NORAD, the North Atlantic Treaty Organization (NATO), cybersecurity, and firearms safety. NORAD Modernization exists beyond the political level, with a growing public and media awareness of the importance of continental defence.

Agile Homeland Defence

NORAD Deputy Commander Lieutenant-General Alain Pelletier spoke of the agile homeland defence enterprise and Information Dominance. NORAD can employ more affordable defeat mechanisms by working with commercial, private, and industry partners. Information Dominance begins with data, and NORAD's ability to respond to future crises will depend on whether Information Dominance can be achieved from sensors, including software and hardware infrastructure.

Ingesting, aggregating, displaying, and processing data quickly will lead to Information Dominance, and ultimately, Decision Superiority. NORAD and USNORTHCOM must leverage commercially-provided cloud based infrastructure and systems for machine learning (ML) initiatives, which will also make threat decision making easier. An all-domain data pipeline is necessary to ensure global integration, and ultimately, battlespace awareness from seabeds to cyber space.

Agile homeland defence must have flexible architecture that can be enabled for rapid expansion and scale, not bound by capacities of current systems. This requires globally integrated effects from allies and partners working together to outpace competitors through strategies, commands, and organizations. Agile homeland defence includes the involvement of both interagency cooperation and government actors beyond those associated with defence.

NORAD and USNORTHCOM has been leading a series of Global Information Dominance Experiment (GIDE) exercises. GIDE is a cost-effective data solution to increase decision space through earlier detection and warning by "enabling cross-Combatant Command collaboration to generate globally integrated effects using artificial intelligence (AI) enabled information." [1] With proper security and data standards across allies and partners, information sharing with bidirectional data flow will allow for joint all-domain operations between NORAD and its allies.

[1] NORAD and U.S. Northern Command Public Affairs, "NORAD and U.S. Northern Command lead the third Global Information Dominance Experiment (GIDE)," 21 July 2021, https://www.norad.mil/Newsroom/Article/2703605/norad-and-us-northern-command-lead-the-third-global-information-dominance-exper/.

Pathfinder Initiative

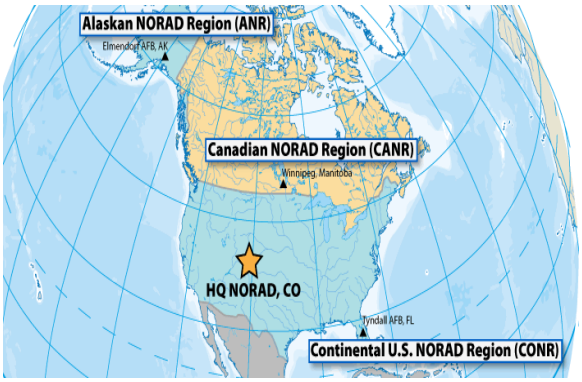
Colonel Robyn Hulan (COO N2X/Pathfinder), the Canadian Team Lead for the Pathfinder Initiative at NORAD headquarters in Colorado Springs, presented an update on the program. Pathfinder is an innovative initiative led by NORAD and USNORTHCOM that is defined as a "technology leap for homeland defence command and control systems." Pathfinder has vastly increased the velocity of time critical processes by removing numerous human interactions in the decision-makers OODA Loop ("observe-orient-decide-act").

Pathfinder is changing the relationship with our data. Due to changes in technology, NORAD must adopt new methods of analysis that provide analysts with more information from more sources to create Decision Superiority in conflict, crisis, and competition. Pathfinder can process more sensor data, allowing the program to detect more information buried within the data. This has repurposed the existing sensor architecture. Pathfinder seeks to transform data from an independently managed data system, constricted by silos, into a data fabric that can be analyzed at the velocity of need with unbounded scale. Pathfinder is creating a new homeland defence cognitive ecosystem to support NORAD modernization efforts.

The initiative is heavily focused on data engineering and automating ingestion to human-readable language. Once this process occurs, machine-learning models can be built to create algorithmic processes. Pattern of life and anomaly detection will lead to Information Dominance objectives. Beyond Information Dominance, predictive and prescriptive analytics come from Pathfinder and the GIDE exercises. This entire process, and Pathfinder writ large, seeks to give the Commander Decision Superiority.

The United States has a robust, secure cloud architecture at all levels of classification. User authentication and accreditation gives military officials proper access to the data they require, based on rank and security protocols. This program also provides flexible response options at strategic, operational, and tactical levels for the Commander. The Pathfinder Initiative will be key in NORAD modernization efforts in both Canada and the United States.

USNORTHCOM's Evolving Threat Assessment



Colonel Matt Eberhart, Ph.D., U.S. Army and Special Assistant to the Commander, NORAD and USNORTHCOM, gave an overview of USNORTHCOM's evolution relative to expanding strategic options and priorities in the current threat environment. USNORTHCOM became operational on 1 October 2002, following the 9/11 attacks. The number one priority mission was to combat Violent Extremist Organizations and prevent another 9/11-style attack. This is in stark contrast to NORAD's prior focus on long-range Soviet bombers. In 2005, USNORTHCOM also provided Defense Support of Civil Authorities in response to Hurricane Katrina in the Gulf of Mexico. The 2018 U.S. National Defense Strategy stated that "it is now undeniable that the homeland is no longer a sanctuary". Peer-level competitors have global reach, which significantly impacts the information environment as well as the manner in which data are disseminated.

The two principal competitors to the United States – namely China and Russia – pose a variety of challenges and threats that decision-makers

have not seen. These threats include Counter-Space, Ballistic Missiles/Hyper Glide Vehicles from peer-states, Ballistic Missiles from rogue states, Cruise Missiles and Hypersonic Cruise Missiles, Cyber-warfare, and Violent Extremist Organizations. These will challenge the forward-operating model of deployment (i.e., deal with threats far from the continent) and create greater risk towards critical infrastructure located in the homeland.

NORAD must prioritize missile warning, missile defence, cruise and hypersonic cruise missile threats to close capability gaps and provide a credible deterrence moving forward. General Van Herck (Commander of NORAD and USNORTHCOM) states that he does not have many viable strategic options available below the nuclear deterrent threshold. The traditional option is to defeat in conflict at the tactical level, but with the speed, accuracy, and multi-domain aspect of threats today, this is very difficult. General Van Herck has requested strategic options focused on Domain Awareness and Information Dominance to increase time in the decision space, move further left of bang, and improve the ability to compete and deter.

NORAD and USNORTHCOM's ability to Deter in Competition, De-escalate in Crisis, and Deny and Defeat in Conflict requires: Global Integration, Domain Awareness, Information Dominance, and Decision Superiority. To compete, deter, and fight globally, regional constructs in the organization of strategy, plans, and global force management will be requirements. Domain awareness is the tool to achieve this. A globally integrated, layered defence with a sensor grid from sub-surface to on-orbit, and everything in between, is necessary. The key will be the ability to unlock the data and ingest it into a common data architecture. Currently, approximately 98% of sensor data is left on the "cutting room floor," because the sensors were designed to look for specific targets and profiles in the era the sensors were implemented in.

Information dominance can be achieved through this unlocking of data in an all-domain awareness environment that includes global sensing. If the problem is treated as a data issue, then software solutions can be used to attain Decision Superiority. Software solutions can increase time in the decision space. Tying all of the joint partners together in a "single-pane of glass environment" with the same, globally-collaborated information across various seams, is vital.

In 2015, a gyrocopter landed on the White House lawn. This, along with similar events spurred the development of the Pathfinder Initiative. This included bringing in modern data algorithms, machine-learning, and data analytics to unleash the power of Pattern of Life (PoL) detection and anomalies earlier to increase time in the decision space.

Decision Superiority results from global integration, all-domain awareness, and information dominance to create more time at the tactical, operational, and strategic levels in the military, economic, and diplomatic spheres. Messaging in the information space can change the trajectory in a conflict. In short, All-Domain awareness leads to Information Dominance,

which creates Decision Superiority for decision-makers at the highest levels. Ultimately, the three objectives are: 1) Improved decisions in competition, crisis, and conflict; 2) Proactive options to deter, deny, and if required, defeat; 3) Global Integration across tactical, operational, and strategic levels.

Opening Remarks from the Information Dominance Panel

Tom Karako, Senior Fellow, International Security and Director, Missile Defence Project at CSIS began his presentation by discussing Russia and China's capabilities beyond traditional Intercontinental Ballistic Missiles (ICBMs). In 1991, the United States placed the former Soviet Union on notice that Washington had the aspiration to go after space-based ballistic missile interceptors. Today, the threat to North America has become lower-altitude and endo-atmospheric with greater maneuverability. This is due to the proliferation of cruise missiles and the appearance of hypersonic gliders and undersea capabilities. The geopolitical, technological, arms and missile control defence landscape has created a new era of missile warfare, according to the planning guidance of General Berger, the Commandant of the United States Marine Corps.

In the Cold War, Soviet bombers and ICBMs created a distinctly less complex threat environment. Today, new threats means that information sharing needs to be more prompt between commands and include all domain information. Existing sensor capabilities need to detect lower-flying threats and Karako suggests elevated-sensors is the solution. Towers, mountaintops, or on aerostats (such as the now-cancelled JLENS project) are critical to develop and act on information in a timely fashion.

Julia Scouten, Senior Manager, Cyber Security Team at KPMG states that Information Dominance comes from achieving the best practices in securing data and cybersecurity. Knowing what data exists, where it is located, and who has access to it, is vital to trusting the existing data when it is available to decision makers.

Chris Pogue, CEO of Thales Canada reaffirmed Scouten's remarks that data, access, and security are crucial across the board. It is partially a data issue when connecting new and legacy sensors together, but the use of data through artificial intelligence (AI) may be more important. Trusting data, effectively sharing, and securing this information are important components. There are various commercial technologies (an example

is cloud computing) that the military can leverage for its benefit.

NORAD and All-Domain Awareness

There was discussion centering around the connection between Domain Awareness, Information Dominance, Decision Superiority, and the need for NORAD to be given an all-domain mandate.

Karako suggested that this issue is not just a NORAD and USNORTHCOM issue. It is widely agreed upon that the homeland is no longer a sanctuary. Proliferation of Unmanned Aerial Systems (UAS) and Cruise missiles is most likely the reason why NORAD and USNORTHCOM is taking the lead on Information Dominance. Furthermore, information sharing is a global problem and the lessons learned can be applied to other combatant commands and possibly applied to the entire UCP.

Scouten stated that at the core of data transformation, good data must be used so that decision-makers can trust it and get the entire operating picture. If the intent is to have multi-domain data, then a larger mandate may be necessary. Artificial intelligence and machine learning are only as good as the available data. Mr. Pogue said that good artificial intelligence requires good information architecture (IA), and that this is an all-domain problem. Common data

standards and the common data environment may ingest data from non-traditional sources, such as social media, to get left of launch. This is a system-of-systems' problem because of the presence of so many layers, sensors, components, and more on their own life cycles. Absent government investment, there will be a gap and flaw somewhere.

Colonel Eberhart interjected, stating that NORAD's area of responsibility as it relates to aerospace defence is North America. Information Dominance will rely on U.S Indo-Pacific Command (USINDOPACOM) and U.S. European Command (USEUCOM) and Space Command sensors. USNORTHCOM's ability to retrieve globally integrated information to the comprehensive multi-domain problem is beneficial to North American defence.

Information Dominance vis-a-vis Five Eyes and a hypothetic multi-national NORAD

The panelists discussed the potential for future Five Eyes cooperation in terms of Information Dominance and where limitations fall (technological, policy, etc.). Karako said that this depends on the problem that is trying to be solved. NORAD is of course about the defence of North America and there are numerous gaps and seams between NORAD and USNORTHCOM as well as between the other combatant commands and allies. Decision-makers in NORAD and USNORTHCOM think differently about the aerial threats from the North and from the South. Therefore, there should be close linkage between NORAD and USNORTHCOM and U.S. Southern Command (USSOUTHCOM).

According to Scouten, it all depends on what the intent and strategy is relative to the overall objective. In this hypothetical scenario of

Information Dominance vis-a-vis Five Eyes, the type of data and information needed to achieve that objective will be of great importance.

Chris Pogue stated that the greatest challenge lays between interfaces and seams of engineering design. If one thinks it is an information/left of launch problem, then NORAD/USNORTHCOM will have to widen its arc and Five Eyes is a good representation of traditional working allies that have expertise to offer and value to gain. Cyber actors around the world could impede the OODA Loop, changing the threat environment and course of action rapidly. The paradigm of information dominance must be considered.

NORAD and the construct of U.S. Unified Command Plan for All-Domain operations

The Chairman and Vice Chairman of the Joint Chiefs of Staff are always looking at the structure of the UCP, especially with the inclusion of the new Space Command. The geographic areas of responsibility mandated to each combatant command may be problematic because the future war fighting concepts do not have battle lines. This is much of what the NORAD and USNORTHCOM GIDE exercises seek to explain.

Ultimately, adversaries are not restricted by geography and are always seeking to exploit gaps and seams. The ecosystem of NORAD and USNORTHCOM comes down to who and what are the threats, but not necessarily where they are located. For instance, are nation-states seeking to damage supply chains and data infrastructure? Another consideration is the possibility of an insider threat with access to a plethora of information and an alternative motive. Organized crime and state-sponsored actors are blurred and inherently tied together.

Deniability about who perpetrated an act in the cyber domain would create mass confusion when superimposed on a global information grid protecting the homeland. Chris Pogue argued that we need to keep an asymmetric advantage with the technology. Attempting to solve problems with too much technology can be ineffective. Quantum sensors are showing promise in how we collect information and create evolution to the systems-of-systems architecture that includes legacy sensors.

Private Sector Response to Military Needs

It is not clear that industry is necessarily poised to solve the problem of information sharing and its effectiveness. Faster decision-making space may be more valuable than more data. Investments in augmented and artificial intelligence means industry can bring unique and differentiating value. Industry is already keeping pace in adoption and implementation of explainable artificial intelligence and cloud computing efforts (already present in NATO through Thales Nexium Defence Cloud) such as evolutionary Thales Defence Cloud Edge.

Julia Scouten asserted that technology is not the problem, but rather, people and processes are. If there is no proper governance structure to manage it, there is no way to keep pace with industry and public sector. When it comes to digital transformation, it is people centric with a focus on process. Creating a governance structure and foundation is the more difficult challenge on the digital transformation journey, but we tend to focus more on the technology itself.

The gap between soldiers and think tanks is still an issue. Information Dominance has been achieved in other sectors such as financial or rail sectors, but not yet for the military. Early-

engagement is vital. The key between government and industry is relationship building early and often. Conversations must be had to identify issues and key aspects of problems together, not just through government requests for information (RFI).

The broader industrial base such as hypersonic and microelectronics/semi-conductors will be important players in NORAD modernization. Industrial pushing and government pulling regarding all types of sensors for the North Warning System (NWS), or new systems will occur. Canada has bought the AEGIS Combat System (ACS) from the United States for more air-tracking capabilities, and this represents an important commitment to modernizing its early warning system.

Areas for Resource Allocation

NORAD Modernization is going to be a large enterprise where all funding will not happen all at once. As Tom Karako said, while our domestic military acquisition and procurement systems offer frustrations, presumably our adversaries have the same challenges, which can be leveraged to our advantage. Canada and the United States are Arctic nations and need to be present in the north to keep an eye on Russian and Chinese actions. This includes presence in asserting sovereignty and icebreakers, which play a pivotal role due to melting ice.

Fixing the legacy problems from the NWS, and inclusion of new space-based and elevated sensors should be prioritized. According to Scouten, people are the greatest assets and creating a pipeline of expertise will pay dividends down the road. Data analyst roles and scientist training programs (AI and ML) on both the civilian and military sides need to be created and fostered. Finding people, training them, and retaining them with the right skillsets is necessary.

Personnel challenges (especially senior talent) could be solved by the military creating a higher calling or purpose that private industry cannot achieve. Ingesting legacy systems to test legacy sensors into a new system and ensuring a Common Operating Picture (COP) and data collection (space, quantum, etc.) is of great importance. Investing in information architecture will produce long term dividends. Chris Pogue further emphasized the necessity for icebreakers and sovereignty assertion throughout the North American Arctic.

Cloud Architecture and Decision Superiority

Policy-makers must think about how to acquire software with a procurement system that was built to buy hardware in the industrial age. The public policy environment is having tremendous difficulty attempting to keep up with rapid technological advancements.

One cloud architecture for all is not an accurate representation. Regardless of what architecture is chosen, you will always be responsible for data inside and who is granted access. There must be a foundational structure of what data are present, who has access, and how to categorize the data, before deployment.

There is a need for trust in any kind of solution. Decision-makers must be able to trust the data, as well as the safety and security of that data. If we want to put time back in the OODA Loop, decision-makers must be able to trust the data being provided to them. Even 5 minutes is key before conflict. In short, trusting information, effective use of cloud computing and security measures, and adding time to the OODA Loop is what Artificial Intelligence can help with.

About the Conference of Defence Associations Institute

Established in 1987, The CDA Institute is a charitable not-for-profit policy centre that is building a community of practitioners, scholars, students, and policymakers who care about Canada's role in the world and are keen to learn from one another to help promote a rational and evidence-based approach to Canadian security and defence. Our varied research activities, events and publications are disseminated amongst various audiences: Canadian and International public, media, policymakers, the military, the diplomatic corps, business community, and academia. As a charitable not-for-profit policy centre, we depend upon the support of Canadians to fund our education, research, and recognition activities. We are building a community of practitioners, scholars, students, and policymakers who care about Canada's role in the world.

Special thanks to our NAADSN rapporteur:
Nicholas Glesby