USE OF A DRONE FLEET IN THE ARCTIC

A Path Forward

The Ukrainian conflict has shown the efficacy of drones in maritime warfare. They have successfully engaged forces considerably more significant than themselves. This discussion paper presents an example of an approach that warrants consideration for Arctic Defense.

Contents

Limitations OF Examples

This discussion paper identifies specific technologies. This is intended to be illustrative and not necessarily prescriptive. If this approach is used, the technology employed should be based on a combination of operationally driven factors directly aligned with the Arctic operating environment. The examples of specific drones presented here are intended to guide the reader towards specific examples that have been operating successfully in other theatres.

Purpose

This document presents a different starting point for considering another option for Canada to maintain its Arctic sovereignty.

Background

With the Arctic coming under increased scrutiny, Canada must respond in such a way so as to ensure its sovereignty is respected while not posing an overt threat to its neighbours. With foreign states eyeing our resources hungrily, shipping routes opening, and certain states seeing our current position as an opportunity to threaten our security, there is little room for half-measures.

Goals and Objectives

Our goal is a secure and sovereign Arctic. Securing territory invokes holding or possessing that territory. “Sovereignty” means that Canada is the sole entity controlling within that space. It sets the rules, and no argument against the contrary is brooked.

How would we assess that these goals are being achieved? If the goal involves a “secure” and “sovereign” Arctic, we can use the attributes associated with those criteria to support a claim that the goals are being met.

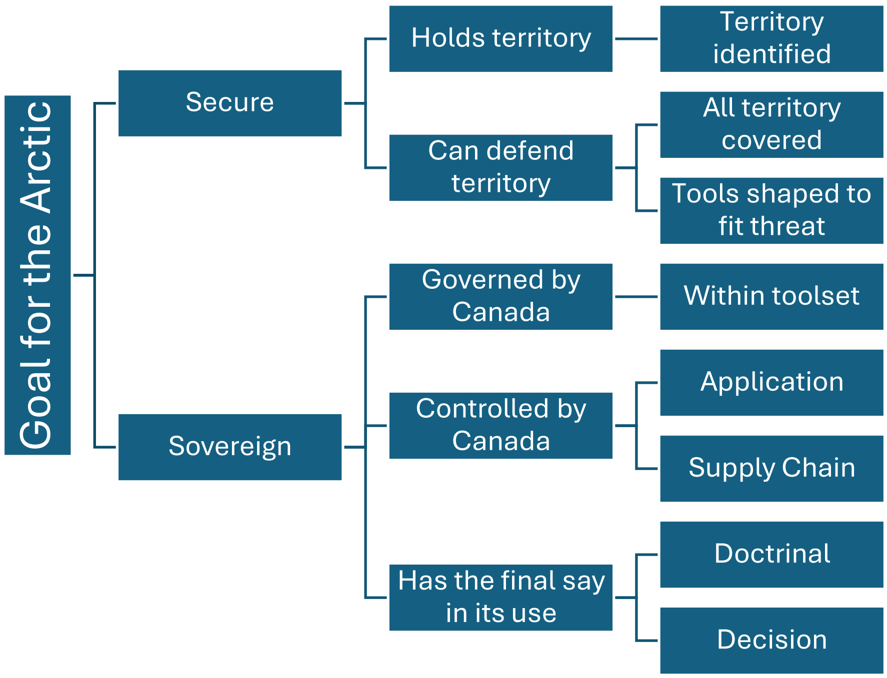

Figure 1 - Breaking down the goals

These goals can be resolved to a series of objectives that, when met, can be consolidated to argue that the system has achieved its goals. These include the following:

Sub-Goal	Normal Conditions	Contested Conditions
Territory Identified	Not system tied	Not system tied.
Territory Covered	The system's performance reaches beyond the boundary of the territory identified.	The system's performance covers the boundary from multiple points
Shaped to Fit Threat	Payload (size and type) can be expected to remove enemy combatant from operations.	The number of drones brought against an enemy combatant can saturate defenses.
Governed by Canada	Not system tied	Not system tied
Controlled by Canada – Application	The system's functions are directed by control centers in Canada	The system's functions are protected against hijacking by those not in authorized control chain.
Controlled by Canada – Supply Chain	All persons, assets, facilities, information, and supporting services can be obtained by Canada from trustworthy parties	All persons, assets, facilities, information, and supporting services are delivered by Canadian companies and functions can be performed by internal resources if necessary.

Table 1 - Goals to more measurable objectives

Problem and Solution Considerations

We face several challenges. First we are a smaller force. This is not to critique those in the military. It is simple numbers: our competitors or threat actors have more. Even if we did start to shift the balance with new submarines, destroyers, replacements for the MCDV, and brought all the AOPS online, we are short sailors. Second, we lack infrastructure. If we are sustaining a capable force, we will need to improve our transportation, communications, and energy resources in the area. Third, any of this activity takes place under challenging conditions. Whatever equipment is brought to bear will be tested between sea ice, harsh conditions, and severe weather.

What do we have that can aid in resolving our challenge? We can develop technologically advanced equipment, possess good engineering skills, and a have host of maritime research centers ranging from basic university research through modelling/simulation, to test ranges for autonomous vessels.

The idea presented below faces challenges, most likely in terms of the colder weather and sea ice. Again, those are known conditions, and it is a matter of overcoming them. It is another story if the waters are clear of ice. Canada is no stranger to this particular challenge and the answer may be guided by the Concept of Operations.

The second challenge involves the threat actors involved. In this context, we can assume that the adversary or threat actor would be able to detect, track, and act against multiple targets. We should assume that modern warships would be able to track the entire force at significant distance. When addressing this, the Concept of Operations would be that the number of targets being brought to bear against the adversary would saturate its defences. If ten are sent against the target, we only need one to get through but the target needs to defend successfully against all ten (meaning complete neutralization before the attack reaches the hull).

This raises the question of supply chains and the resupply of positions where the devices would be launched. The lessons associated with the 155mm shells in Ukraine conflict should not be lost here. That lesson was that many were needed, stockpiles were depleted quickly, but the rate at which the shells could be manufactured fell short of demand. Ideally, this solution would not fall into the same trap meaning that (1) an adequate stockpile of weapons could be managed for a reasonable cost and (2) second-line stockpiles could be established in safe areas that could be moved quickly into place, and (3) Canada would maintain an ability to manufacture replacements at or above the rate that they would be expected to be used.

Geographical Factors

We also have the advantage that the Arctic has relatively narrow transportation routes surrounded by challenging coastlines. The Roman legions were considered invincible until they marched into the forests of Gaul, where the battles were suddenly close- fought. The coastlines and smaller waterways that cover this area may well be analogous.

Figure 2- The coastline and its interconnected waterways and complex topography

Previous Success of Drones in Ukraine

The war in Ukraine has shown us a few things about naval warfare. Introducing and refining how to use drones in that conflict have changed some maritime conflict dynamics. We should pay attention to that. We should also pay attention to the changes in those technologies. We may have started with relatively primitive remote-controlled vessels delivering a charge to systems that can actively defend themselves and operate autonomously under certain conditions.

The Magura V drone has a range of about 800 km. The circles in Fig.2 below have diameters of approximately750 km, and are drawn from locations where we have an existing presence: Mould Bay, Resolute, Arctic Bay, Iqaluit, Cambridge Bay, Coral Harbour, and Inuvik. Consider that each of those points has a detachment of personnel capable of managing a fleet of 10-12 Magura V or Sea Baby drones that have been adapted to operate in colder weather.

Canada also has domestically produced aerial drones or Remotely Piloted Aircraft Systems (RPAS) that can achieve the same distances with a payload of over 250 kg. This is slightly less than the

300kg carried by the Magura 5 drone and significantly less than the one tonne considered for the Sea Baby. This is still enough to cause considerable damage to most warships.

Concept of Operations

Our Concept of Operations looks to accomplish two things. The first is to achieve a level of deterrence. This can be described as the condition in which an adversary is discouraged from committing an act through either outright fear or by instilling enough doubt that the course of action being discouraged could result in unacceptable consequences. Our second aspect involves ensuring that this is seen in terms of what it is – a defensive tool. It should be difficult to consider this tool in an offensive context. The intent here is not to have the system become a provocation or an excuse for action against Canada.

The general operations can be looked at in terms of Identification, Protection, Detection, Response, and Recovery. These include the following:

- **Identification**: This would involve all surface vessels seeking to pass through Canadian waters or operate in Canadian waters, regardless of their authorization.
- **Protection**: would include a series of legal controls (reporting requirements for shipping), this system, and ensuring that ships in the area were aware of the consequences of going outside of the rules.
- **Detection**: This would involve being able to identify a unique vessel in terms of its identity, location, heading, and that it was not operating in alignment with Canada's requirements.
- **Response**: This would likely involve a rapid escalation through communications, "warning activities", and (if necessary), the defensive action of launching the action against the offending vessel.
- **Recovery**: The Arctic is an environmentally sensitive area. The response should seek to limit damage to the extent reasonable to achieve Canada's aims (for example, disabling the vessel versus sinking it). Ideally, the capability should be able to assist in the assessment of damage and even seeking to remediate its subsequent or follow-on impacts (such as spills).

This would begin at either end of the entry to the Northwest Passage. Our current sensor network (including space-based monitoring) could alert to traffic in the area that warrants attention. Reaching out to those in the area, including the Arctic Rangers, with reporting requirements would also support this. The goal here is to have "as many eyes and ears" looking and generating a list that is sorted into what traffic is authorized and which may warrant response. The first line of the tripwire would be outside the coverage zones (see below) and would likely be tied to the waters subject to the Exclusive Economic Zone and Coastal Shelf Limits.

Where a ship has indicated that it intends to transit the waters (such as through the UNCLOS Right of Innocent Passage), details about the ship (photos, description, markings, contact details, etc.) are communicated to those responsible for targeting and preventing unintentional attacks. This step could easily follow normal reporting requirements currently covered under the Pre-Arrival Information Reports covered under Canada's Marine Transportation Security Requirements (Section 221). These would then be processed as they are today.

At this point, the discussion shifts to the response phase of the activity. At this point, it is assumed that the threshold has been breached that would see the deployment of drones. As noted above, this would likely involve an escalation of force that could, if all other measures fail, ultimately lead to an action against the vessel. This would likely involve the following:

- **Step 1**: communication and warning through radio or similar normal communication channels to advise them of the need to comply or face consequences.
- **Step 2**: Show of presence through a single drone being launched with the intent to be detected. This would essentially show the offending vessel that it is now "on a clock" to comply.
- **Step 3**: Final warning and activation of centers where actions would be launched from.
- **Step 4**: Action taken by launching an action against the ship with the intent to stop the offending action.

This may involve a combination of surface-level drones and remotely piloted aircraft.[1] These could be launched from two or more centers. Those drones on the surface would leverage the drone's autonomous functionality to approach the vessel, while on board AI would maintain drone spacing and speed that would make it more difficult for the guns on the incurring ship being attacked to acquire, lay on, and fire upon the drones. Similar features could be built into the aerial drones.

The concept here is relatively simple. It takes time to identify a threat, turn a weapon against the threat, and then neutralize the threat. Leveraging AI and situational awareness would allow the "swarm" to maintain its configuration in such a way that the next immediate threat requires as much effort as possible (i.e., movement of gun, etc.) to be effective. The key concept involves the saturation of ship defences. If enough drones approach a ship from enough different angles, a few will manage to get past its defences. Those would have sufficient impact to cause considerable damage to the vessel in question.

[1] There are STOL RPAS capable of a 280 kg maximum cargo load with a range of 800 km.

Should this scenario involve a higher intensity contract, one might consider replacing standard high-explosive squash head warheads with thermobaric warheads to increase the damage to the target.

Again, the ideal situation would involve the use of only that force necessary to bring the ship back into line with Canadian requirements. This does not mean that Canada would project an unwillingness to escalate down the entire chain. It only means that the “off ramps” are built into the system in such a way that Canada achieves its ends without *necessarily* having to resort to potentially damaging measures.

This action would also necessitate the activation of environmental containment crews in the area. Ensuring that survivors are “rescued” and that environmental damage is contained becomes the focus of activity. In this case, the drones shift from an “attack” mode to a “surveillance or reconnaissance” mode. A secondary wave of drones may be provided to assist responding vessels by helping in towing booms, etc.

Refining the Concept of Operations

The next figure shows one option. This may, or may not, be an optimal approach but is presented as *one of a number of potential workable approaches*. Given the transportation and other challenges in the area, it may also be prudent to build a less predictable system where key control points, launching points, and other aspects of the system could be made more variable (unpredictable). Structuring the command-and-control functions using a resilient architecture and topography would make the system difficult to take down with a pre-emptive strike unless all centers were taken down simultaneously.

Figure 3 - Sample coverage at a radius of around 750 km

Part of this resilience would see the command-and-control functions for these drones being able to be passed across the various communities or possibly back to a national center. Should the control center in one area being neutralized, then a "backup" center would then take control to maintain the capacity.

Sustaining the drone capability at each location would require a small cadre of personnel able to monitor, maintain, test, and (if needed) deploy the drones. Each of the centers identified already has small communities and infrastructure. While it would be tempting to centralize personnel for cost-efficiency purposes, this should not be done in a way that reduces a set performance threshold for the ability to put any step in the plan into operation.

The concept of resilience stretches from the upper levels of the command-and-control function to the asset itself. In addition to the discussion above, the drones themselves could be fitted with defensive or offensive tools that would make them more difficult targets. For example, drones in Ukraine have been fitted with rockets or machine guns that can be used to defend the drone. These kinds of tools could be put in place to force warships to "clear the decks" during the final phases of the attack.

Cost

These costs are provided for discussion purposes and should be considered rough estimates.

What would the cost be? There are seven zones identified and we assume eighty-four drones are a "basic load." At $300,000 Cdn per drone, the total for drones is just over $25 million Cdn. There may be additional cost associated with licensing (paid to Ukraine in terms of unlimited license for use of the design) or in terms of having persons from Ukraine able to help with establishing Canada's local production capability.

The cost of supporting the distributed centres can also be estimated. We know from the Nunavut 3000 project that the cost an estimate of $1 million (Cdn) per unit for construction could be considered reasonable as a starting point. So, let us just put forward an estimate of $200 million Cdn[2]. This would include the facility storing the drones (including over winter), maintenance equipment, and able to support the cadre of personnel.

Upgrading the transportation, energy, and telecommunications infrastructure at those sites would be required. We would be able to establish an initial operating capability relatively quickly. Each site has an airfield runway of over 3500 feet in length, making them capable for Hercules and Globemaster aircraft use. Satellite communication is available in the area but would likely benefit from greater Canadian control. The challenge would largely lie in energy considerations with a large number of these communities relying on diesel generators for their power production.

These infrastructure upgrades would have both civilian and military applications and would likely involve an incremental approach. Wind-based generation (understanding that solar is an option in the summer months but not so much in the winter) or (as technology advances) small scale nuclear distributed from the mainland could facilitate the deployment and sustainability of this kind of infrastructure.

[2] To put into context, this total represents about 1% of the cost of a River Class Destroyer (if based on a $22 billion Cdn price tag).

The portion of the work intended for use by the military falls within the rules for the 2% GDP NATO contribution. These efforts can be counted towards two national goals: opening the Arctic and towards meeting our long-overdue defence bill.

Supporting Hubs

Canada has identified three hubs for military activity in the area (Inuvik, Yellowknife, and Iqaluit). Of these, the likely preferred alternative would be Yellowknife as the inland second-line supporting hub due to its proximity to multiple transportation routes, supporting supply chains, infrastructure, and so on. Iqaluit and Inuvik would be assigned secondary roles, largely due to their exposed positions on the flanks of the system but also in terms of their more limited infrastructure.

These hubs could be the staging area for the supply chains supporting these bases. The Magura 5 weighs about 1000 kg but adding an additional 500 kg to cover the weight of packing, spares, and whatever else needs to be shipped would be prudent. We have already noted that each of these communities has airfields capable of handling either the CC-130 or CC-177. The Hercules aircraft can carry a payload of up to 21,000 kg. One Hercules aircraft could carry the weight of a full complement of 10-12 drones. Dimensionally, one drone package would consist of a length of eighteen feet, a width of five feet, and a height of approximately three feet. Resupplying the entire complement of drones would require one trip for a CC-177, but two trips for a CC-130, given the close alignment between the space required and the available space. For the CC-130, most of these trips would take less than three hours in the air (assuming a flight speed of 660 km/h and a route shorter than from Iqaluit to Mould Bay).

Additionally, Canada has several centres that may be useful in this context. Several centres suitable for the development and testing of autonomous vessels are currently in existence. Canada also has the availability of centres such as NATO DIANA and COVE that can be leveraged. These centres are already functional.

Conclusion

This document is intended to promote discussion on alternatives that fall outside the normal doctrine or approaches being discussed with respect to assuring Canada's Arctic sovereignty. It is intended to provide enough detail to be meaningful but leave enough flexibility for adjustment based on conditions, national priorities, and what is achievable. The current lack of infrastructure and Canada's emerging new doctrine in Arctic defence can be turned to our advantage. There is little infrastructure in place to remove and doctrinally, we are not necessarily tied to only one approach.

There is little doubt that Canada's position militarily is that of the "underdog." That being said, mass is only one factor on the battlefield. Additionally, periods of significant need can lead us to make important innovations. We should remember the dictum "if you are planning to get into a fair fight, then you are doing it wrong."

About the Author

Allan McDougall has focused on critical infrastructure protection and assurance over the past 30 years across military, public service, and the private sector. These have included within the Department of Fisheries and Oceans/Canadian Coast Guard, Transport Canada (as the Senior Inspector for Ports), and the Canada Border Services Agency. Within the private sector, he has worked to support transportation networks and maritime operations both domestically and in higher-risk environments. He is a founding member of the International Association of Maritime Security Professionals and one of Canada's original trainers under the IMO Train the Trainer program. He has worked across the lifecycle from design activities within the CSC Program at Irving Shipbuilding.

Allan has co-authored four books on Critical Infrastructure Protection and one book on Transportation Systems Security, which focus on establishing and managing resilient networks. These works have been used as graduate texts at several universities.

Allan holds an MA in Security Management from the American Military University (focusing on autonomous shipping) and a BMASc from the Royal Military College of Canada. Additionally, he holds a BA from the University of Western Ontario. He holds several security-related certifications, including the Certified Protection Professional (ASIS), Physical Security Professional (PSP), Professional in Critical Infrastructure Protection (PCIP), Certified Master Anti-Terrorism Specialist (CMAS), and Computer and Information Systems Security Professional (CISSP).

Allan is a director at the National Center of Excellence and Innovation in Maritime Security and a Senior Security Program Manager at ADGA, located on the Eastern Shore of Nova Scotia.

About the National Center of Excellence and Innovation

Founded in 2024, the National Center of Excellence and Innovation is a multi-disciplinary focal point for communities coming together to address complex maritime security challenges. It draws together academics, practitioners, and others who have related experience ranging from law enforcement to the impacts of severe weather and changing ocean conditions. You can visit the website at https://marseccoe.com.