POLICY PRIMER

NAADSN
North American and Arctic Defence and Security Network

naadsn.ca

June 29, 2021

NORAD Modernization: Considering the Threat of Small UAS to (Integrated) Air and Missile Defence

Christopher Verklan
NAADSN Graduate Fellow

The future of North American defence has been debated at length by scholars and policymakers alike during this latest round of modernization, with many arguing that the resumption of great power competition and the emergence of new threats requires new capabilities and capacity to meet them. Unfortunately, the current discussion, while focusing in on emerging missile threats, has overlooked the emerging use of small uninhabited aircraft systems (sUAS) by state and non-state actors – and the threat these pose to air and air and missile defence systems. This policy primer aims to address this gap in understanding as it relates to the North American Aerospace Defence Command (NORAD) by providing an overview of sUAS and highlighting initial policy implications that can be further developed in the future. Overall, the main conclusions of this primer are that the land-based radar systems currently in use by NORAD are vulnerable to sUAS, and that NORAD should work towards creating a resilient integrated air and missile warning system that leverages air power and non-kinetic forces to mitigate the effects of this threat.

Introduction

The modernization of North American defence has been examined by policymakers and academics alike for the past two decades, with the North American Aerospace Defence Command (NORAD) being one of the main focuses of this analysis. Following the 9/11 attacks in 2001, then Secretary of Defense Donald Rumsfeld proposed that NORAD be transformed into a multi-domain defence command.[1] While this did not occur, five years later the binational NORAD agreement was signed indefinitely with the addition of a maritime warning mission.[2] Since the implementation of these changes to NORAD, there have been no subsequent alterations to the binational organization's mission-set, although research on the future requirements for continental defence and NORAD's role in this has continued on. The most recent wave of research on the subject began with the commissioning of the NORAD Next study in 2013, where Canadian and American policymakers have been at the forefront of determining future defence requirements.[3] Although this study was scaled back in 2015-2016 and replaced by the Evolution of North American Defence study, the underlying premise of the study had not changed, with its subsequent results being presented to the Permanent Joint Board on

Defence.[4] Unfortunately, given the secrecy of the findings presented, these cannot be elaborated upon further here. This, however, has not stopped academics from exploring the issue with leading NORAD scholars Andrea Charron and James Fergusson releasing several studies on the matter.[5] More recently, the Conference of Defence Associations Institute hosted a three-part webinar series on NORAD modernization, with former NORAD commander General (ret.) Terrence O'Shaughnessy and NORAD's Deputy Director of Operations Peter Fesler, releasing a paper on the subject shortly thereafter.[6]

While space precludes an in-depth examination of each of these publications, there are several core conclusions at the center of each of these analyses that should be noted here. First, the actors, as well as the threats posed by each actor, are growing and require NORAD to improve its capabilities and capacity to meet them. Included in this category is the resurgence of great power competition with China and Russia and their development of hypersonic weapons, ballistic missiles, and advanced submarine launched or air launched cruise missiles (SLCM and ALCM, respectively).[7] The emergence of these threats has spurred academic discussion on the issue of missile defence and the requisite enabling factors needed to pursue it. Regarding the latter point in particular, this has led to a focus on the renewal of sensors and adopting Joint All Domain Command and Control (JADC2) to meet this next generation of threats.[8] Although these discussions have been much needed in the current academic discourse, thus far, little attention has been paid to the increasingly important role played by small unmanned aircraft systems (sUAS) in modern combat despite the proliferation of this threat.[9]

Overall, this primer aims to explore the effects of the development and proliferation of sUAS as it relates to integrated and non-integrated air and missile defence, with a focus on NORAD. To do so, this primer breaks down the issue into three sections. The first section provides an overview of the capabilities of this weapons system, defines the mission sets for which these weapons systems can be used for, and highlights future capabilities currently under development. The second section outlines the attributes of integrated and non-integrated air and missile defence systems and the challenges that sUAS pose to both. The last section seeks to link the previous two sections, identifying the implications of this weapons system for NORAD and outlining how it should mitigate this emerging threat. The core conclusions reached by this policy primer are that the land-based radar systems currently in use by NORAD are vulnerable to attack by sUAS, and that NORAD should work towards creating a resilient integrated air and missile warning system that leverages air power and non-kinetic forces to mitigate the effects of this threat.

Modern Small Unmanned Aircraft Systems: An Overview

Modern sUAS, while being an increasingly topical subject, are not a new technology in and of themselves. For example, the Boeing Insitu Scan Eagle used by the United States Department of the Navy has been in use since 2005, with the Marines using this system as an interim platform since 2004.[10] Despite this, the term utilized to describe this weapons system is comparatively new, with the term being introduced in the recently United States Department of Defense's *Counter-Small Unmanned Aircraft Systems Strategy* that was released earlier this year. In this document, sUAS are defined in terms of their size and other capabilities relative to other unmanned aircraft systems (UAS). Accordingly, sUAS are classified as UAS that exhibit a maximum gross takeoff weight of less than 600kg, have a normal operating altitude less than 6000m, and a maximum speed

under 500km/h.[11] As for the overarching definition of what constitutes an unmanned aircraft, this is defined as being an aircraft that does not carry a human operator that is able to fly with or without human control.[12]

Broadly speaking, sUAS can be subdivided into two categories in accordance with their payload. The first category of sUAS is the sensor carrying sUAS, which can carry one of a variety of specialized sensors, with a camera of some sort invariably being included in this payload.[13] This type of sUAS currently dominates the commercial marketplace, with demand from civilian enthusiasts and photographers driving further commercial developments in the area. Perhaps the most noteworthy of these developments are the increased efforts of sUAS companies to improve the imaging capabilities of their respective products, with high end sUAS now boasting 4K video and low-latency high-definition video transmission from up to ten kilometers away.[14] While already a leap ahead of the capabilities of previous generations of commercial sUAS, additional aftermarket upgrades such as thermal imaging, night vision modes, and laser range finders are also available.[15] As for the software enabling the use of these products, these too have become more powerful with time – with some boasting obstacle avoidance, target recognition, trajectory prediction, and high speed tracking features.[16] Although sUAS boasting these capabilities exceed $1000 USD, cheaper alternatives also exist with more modest capabilities, and often come with preprogrammed features to aid beginner flyers.[17] As a result, while not originally intended for surveillance applications, these civilian sUAS have developed into increasingly sophisticated platforms that could – and indeed have – been leveraged by non-state actors to provide intelligence, surveillance, target acquisition, and reconnaissance (ISTAR) capabilities in support of their objectives.[18]

Looking beyond the civilian market, militaries around the world have also adopted sensor carrying sUAS to perform a similar mission-set. However, unlike the commercially available sUAS these tend to have better sensors, communication and navigation systems, and increased endurance. For example, the aforementioned ScanEagle sUAS has an endurance of 18 hours compared to the typical hour-long endurance of commercial quadcopters. Moreover, this system has a communication range of up to 100km, far more than what is available on the commercial market.[19] However perhaps the most important distinction to note here is that military sUAS have greater access to the electromagnetic spectrum, both enabling the longer communications range noted above, and limiting the sUAS's risk that communications could be affected by inadvertent or intentional electro-magnetic interference.[20]

As for the other category of sUAS, this is the offensive payload carrying sUAS, which carries some form of lethal or non-lethal payload. Beginning again with the commercially available sUAS, it should be noted that for these to carry offensive payloads they must be altered from their factory condition. Typically, this is done one of two ways. First, the actor modifying the sUAS can affix a release device to the sUAS such that when it identifies a target with its built-in camera, it is able to release its payload on or near the target. Such modifications have been made by pro-Russian non-state actors in Ukraine who have outfitted commercial sUAS with various hand grenades, thereby creating an improvised air-delivered munition.[21] Alternatively, the offensive payload can also be affixed to the sUAS itself and be utilized on or near the target. In the case of explosive payloads, the sUAS is in essence transformed into an improvised precision munition that can be remotely detonated on or near the human or physical target. This style of offensive payload has become increasingly popular with non-state actors, with the Islamic State having successfully utilized such a system to target coalition forces in Iraq in 2016, for example.[22] Beyond explosive payloads, there is also concern that

these could act to deliver chemical or biological weapons on open-air targets such as large outdoor crowds.[23] That said, the size of the payload, explosive or otherwise, being delivered is dependent on the size and endurance capabilities of the sUAS being used. Thus, given the limited size and endurance capabilities of currently available commercial sUAS, both the range and payload capable of being transported is relatively small.

Similarly, military offensive payload sUAS also deliver their payload in two distinct ways. Looking to explosive payloads, the most common delivery method currently used by military sUAS is to have the payload integrated into the platform and have this payload detonate on or near impact. This type of sUAS, also known as a loitering munition, has become increasingly popular with time for its ability to effect suppression and/or destruction of enemy air defence (SEAD/DEAD, respectively) missions; with the first of these, Israel Aerospace Industry's Harpy, being developed in the 1980s before being publicly revealed in the 1990s.[24] Although data on earlier versions of the weapon is unavailable, the most iteration of this weapons boasts a 16kg built-in explosive payload and autonomous operation.[25] This autonomy, coupled with a communication range of 200km, and a maximum range of 1000km, enables the sUAS to detect, identify, acquire, and destroy radiating targets (such as radar systems) without risking higher-value assets.[26] This functionality is also aided by its small size, which allows it to have radar cross section (RCS) less than 0.5m^2 – that being an RCS smaller than fourth generation aircraft such as the MiG 29.[27] A variant of this weapon also manufactured by Israel Aerospace Industries, the Harop, also fulfils a similar function – except that it is equipped with an upgraded electro-optical sensor suite to better enable ISTAR missions as well as conduct battle damage assessments.[28] Beyond Israel, a variety of other countries such as China, Iran, Poland, Russia, and the United States have also started to manufacture loitering munitions. Generally, the platforms developed by these countries can carry payloads of less than 50kg, have a range of between 5-500km (dependant on size and expected function), and have a low cost per unit.[29]

More recently, however, states have also become interested in developing sUAS with offensive electro-magnetic warfare (EW) capabilities. Unfortunately, little public information is available about these efforts at the time of writing, although it appears that the United States and the United Kingdom have both expressed interest in developing this capability.[30]

Other than simply integrating offensive payloads into sUAS, there have also been limited efforts to attach precision guided munition systems to larger sUAS platforms. The only example of this to date is the Textron Systems Shadow UAS which has been tested with a five-kilogram, laser guided bomb.[31] The lack of further development of this weapons system following this test appears to indicate limited interest in this capability, despite this still being advertised on its product page.[32]

Looking to the future of commercial and military sUAS, several trends need to be considered. First, there are increasing efforts to make sUAS "smarter" through software upgrades in both the commercial and military space. In the commercial realm, these upgrades will likely include further refinements to autonomous functionalities that improve ease of use for both beginner and advanced users. In the military realm, while some forms of autonomous functionality are available depending on the manufacturer, current efforts in this realm are focused on the creation and applications of drone swarming technologies.[33] Second, in both the commercial and military space, further improvements to imaging and communications sensors are likely to

take place – leading to improved ISTAR capabilities. The third trend to be noted is the increasing number of payloads that military offensive payload sUAS can carry. Again, while little information is available on the subject, an sUAS equipped with an EW payload on its own or in a swarm has the potential to degrade enemy radar systems to the benefit of SEAD/DEAD missions. Lastly, given the limited range of sUAS, the development of launch platforms that can forward deploy sUAS would be essential to enable their usage over distance. Initial steps have already been taken in this direction with the most recent demonstration of this being the release of an sUAS from an advanced experimental UAS in April 2021.[34]

The "Emerging" Threat of sUAS to (Integrated) Air and Missile Defence

The increasing proliferation of sUAS among state and non-state actors coupled with the publicity given to this novel weapons system has helped shape the view in the open literature that this platform is an emerging threat to be countered. In reality, however, the concept of sUAS posing a threat to air and missile defence (AMD) is not new. Rather the "emerging" threat facing modern militaries takes its roots in what was faced by Israel's Arab neighbors during the 1973 Yom Kippur War and the 1982 Lebanon War. Beginning with the Yom Kippur War, the Israeli Air Force (IAF) had utilized a variety of domestic and imported UAS to act as decoys to distract and absorb Arab surface-to-air missiles at minimal cost. This enabled the IAF to significantly reduce losses of the more expensive human piloted aircraft while also degrading Arab air defences.[35] In the subsequent war in Lebanon, IAF sUAS would be used to similar effect, except that after forcing the activation of enemy air defences the IAF would then target land-based radar systems with anti-radiation or other precision guided munitions.[36] Sensor carrying sUAS also played a crucial role in notifying the IAF of enemy aircraft taking-off from their bases – allowing nearby surveillance aircraft to relay intercept vectors to friendly fighter aircraft.[37] However, unlike the threat to AMD posed by other sUAS the past, the advent of modern military offensive payload sUAS has changed the nature of the threat posed by sUAS platforms as a whole.

To understand the threat posed by modern sUAS to (I)AMD, it is essential to first understand the limitations of the current air and missile defences being deployed, particularly by the United States. As noted in a Center for Strategic and International Studies report on the subject, there are several core shortcomings of the current air and missile defence systems being fielded by the United States. The first shortcoming is the stovepiping of information that results from the way in which these systems were designed. In the case of the MIM-104 Patriot air and missile defence system this means that for one missile battery to share data with another, said information must be passed from its own engagement control station through the information coordination center before being shared with the desired engagement control system.[38] This current system is inefficient, and as a 2005 report on Patriot performance in Operation Iraqi Freedom noted, the inefficiencies had led to "[a] lack of significant situational awareness in our combined air defense system, which involved major systems such as Patriot, AWACS, and AEGIS."[39] As a result, rather allowing for target information to be shared and assimilated by these other systems, the stovepiping of the Patriot system meant that "a Patriot battery on the battlefield [could] be very much alone,"[40] thereby reducing the capability of the system and increasing operational risk.[41]

The second major shortcoming of current AMD systems identified in the CSIS report is the existence of single points of failure. This issue strongly relates to the inadequately networked nature of current AMD forces, which in practice means that the removal or elimination of several friendly sensor or command nodes from

the battlespace could lead to the demise of the whole system.[42] This shortcoming is particularly problematic given that the United States' AMD systems have increasingly focused on ballistic missile threats from smaller powers. Coupled with the use of directional, as opposed to omnidirectional radars, this leaves the distinct possibility that current AMD systems could be compromised by a cruise missile, sUAS, or other forms of attack from an unexpected heading.[43]

To mitigate these vulnerabilities inherent in the current generation of AMD systems, the modernization of the United States' AMD systems – as well as the modernization of NORAD's capabilities and architecture – has increasingly focused on a distributed approach that embraces the concept of multi-domain battle.[44] This concept of operations aims to synchronize action across the land, air, sea, space, and cyber domains to achieve a desired effect on the adversary.[45] The most important element of this proposed approach is the information grid that links the nodes within the sensor grid, effects grid, and command grid together. This grid enables the rapid flow of information to be spread horizontally, rather that vertically, thereby avoiding the stovepiping of relevant information inherent in the current generation of AMD.[46] The desired effect of this rapid information flow is to enable all nodes within the sensor grid to provide a comprehensive picture of the battlespace that can be leveraged by the effects and command grid. This, in turn, enables increased flexibility regarding which sensors are employed with which shooters in the effects grid. The main benefit of this newfound flexibility is the ability for a given effects node to leverage data from other domains regarding a target – allowing it to use its interceptor missiles at their maximum range or around physical obstructions that would have otherwise blinded the system.[47]

Returning to the issue of the threat posed by sUAS to (I)AMD systems, there is a clear distinction in the level of threat posed to the integrated versus the non-integrated AMD systems. In the case of the latter, as mentioned above, there is a clear risk that the current bottlenecks present in the command and sensing nodes could be exploited by an adversary using a variety of weapons systems. This risk is particularly acute in the case of offensive payload sUAS as these could circumvent the expected approach routes used by missiles and/or use their small RCS to avoid detection by these systems to deliver or activate their payload. In contrast, the threat posed by offensive payload sUAS in integrated air and missile defence (IAMD) systems still exists yet does not pose an existential threat to the system should the attack be successful. This is because unlike the previous instance where the loss of certain sensor and command nodes leads to the failure of the system, in this case, effects nodes are still able to communicate with other sensor and command nodes. As a result, not only is the IAMD system more resilient in the face of this threat, but it also imposes increased cost on the attacker by requiring more sUAS to effectively suppress or destroy the defender's IAMD system.

The Implications for NORAD's Integrated Air and Missile Warning Mission

The increasing adaptation of sUAS, notably offensive payload sUAS, has two core implications for NORAD and the modernization of North American defence going forward. The first and most important implication is that the land-based sensors are increasingly vulnerable to this emerging threat due to their difficulty to detect, identify, acquire, and prosecute. So far this vulnerability has been visible across a variety of systems in recent conflicts such as the obsolescent Russian S-1 Pantsir[48] and S-300[49] in the Second Libyan Civil War and the Nagorno-Karabakh conflict, respectively, and the American MIM-104 Patriot air and missile defence system in its conflict with the Houthis in Yemen.[50] As a result, this represents yet another threat that NORAD should be

considering and mitigating into the future, especially if states continue to increase the range of these systems, develop the capability to deploy sUAS at range via larger air or sea assets, or a combination thereof.[51] This is particularly true as obsolescent systems such as the North Warning System (NWS) currently employed by NORAD suffers from a structure that is stove-piped and threat-centric, exacerbating the issue of single points of failure noted above.[52] Fortunately, NORAD has time to follow and adapt to this emerging threat because Russia, the most proximate of NORAD's state adversaries, has yet to meaningfully develop this technology into a low-cost intermediate-range strike platform as the Israeli's have – choosing instead to focus on developing short-range variants of this this weapons system.[53] As such, current Russian sUAS pose little threat to North American defence outside of Alaska due to its proximity to Russia's Far East. However, Russia's focus on developing short-range sUAS may change in the future with the increasing development and interest of sUAS, notably loitering munitions, by the Russian Ministry of Defence following Nagorno-Karabakh conflict.[54]

The second major implication is that NORAD is finding itself on the wrong side of the cost curve when mitigating the sUAS threat. For example, Raytheon's Coyote loitering munition currently that is currently being tested as part of the United States Navy's drone swarming program costs around $15,000 USD per unit; with future plans to reduce this cost to $5,000-7,000 USD per unit as the system matures.[55] By comparison, the US-made Patriot Pac-2 costs $1 billion USD for the system itself and an additional $3 million USD per surface-to-air missile – meaning that each missile costs roughly 200 times the price of the aforementioned sUAS.[56] While it is unlikely that system will be utilized by NORAD as the organization does not defend against missile threats and is seeking to develop purpose-built systems for homeland defence;[57] it none the less highlights the relatively cheap threat posed by offensive payload sUAS to these expensive weapons systems. This discrepancy has already been noted by several analysts, with one summarizing the current situation as "[exposing] in very stark terms the challenge which militaries face in attempting to deal with the adaptation of cheap and readily available civilian technology with extremely expensive, high-end hardware designed for state-on-state warfare."[58]

Looking to the ways that NORAD can mitigate the threat posed by sUAS to its air and missile warning mission, it should be noted that NORAD has already made strides in to reduce the threat by increasing the capabilities of existing sensors with the help of artificial intelligence (AI). One such effort that has been made public is known as Pathfinder, which uses AI to "[gather] data from multiple distinct military and civilian air domain sensors and, through automation and machine learning models, [produce] a fused common operating picture to improve the reliability of the data and increase the decision space."[59] In doing so, this allows existing military and civilian sensors to utilize data that would have been "left on the cutting room floor and not analyzed or assessed in a timely manner"[60] – enabling the rapid detection of threats that had previously gone undetected beforehand. For example, this AI is stated to have enabled the detection and tracking of sUAS with sensor data from pre-existing United States Federal Aviation Administration radars, and has also been used to analyze historical incidents to detect small aircraft that had previously gone undetected in restricted airspace.[61] Unfortunately, it is unclear how this software augmentation will perform in less dense sensor environments such as that found in the Arctic where the NWS is located, although it will more than likely have a positive effect on increasing domain awareness to some degree.

However, to enable NORAD to continue its mission-set in the face of the threat posed by sUAS, more must be done beyond breathing life into obsolescent sensor networks that may fail due to their age, position, or

technical obsolescence.[62] In this respect, there are two lines of effort that should be pursued by NORAD. The first line of effort should seek to use the limited range of sUAS against themselves to outrange, or at minimum force the launch of the sUAS at range, with the goal of: (1) deterring the use of sUAS for hostile or covert acts to begin with, (2) minimizing their time on target to provide ISTAR and potentially find and prosecute targets, and (3) allowing for more time for NORAD to detect, identify, acquire, and mitigate the threat in an appropriately deemed manner. To enable this to occur, NORAD first requires an improved sensor network that can detect sUAS launch platforms and the sUAS themselves at range, thereby providing the foundational capability to pursue these three goals. Also, this sensor network must be both layered and distributed to enable this system to degrade gracefully rather than fail at the stovepipes should successful attacks occur.[63] To the organization's credit, its leadership appears to be favoring this approach in public discussions in the academic sphere, ensuring that the revitalized northern sensor system is able to ensure its deterrence by denial posture and improved domain awareness despite the threat posed by sUAS.[64]

In addition to the distributed and layered structure of the sensor network, consideration of the sensors that make up this network should also take place. Overall, the sensors required to detect, identify, and acquire will likely need to be twofold – with the search and detection of sUAS utilizing "wide-area, lower-resolution sensors… to cue higher-resolution sensors to track and identify them."[65] As for the specific type of sensors required for these functions, a recent RAND Corporation report notes that inexpensive thermal imaging sensors are capable of detecting battery-powered sUAS, and that low-cost electro-optical and infrared imaging sensors can be used to detect, identify, and track targets at range.[66] This report also notes the utility of radars in detecting and acquiring sUAS at short and long ranges, as well as the importance to have the adequate number at the right frequency to enable these functions.[67] Unfortunately, this report does not elaborate on the best location for these sensors – be it in the sea, land, air, or space domains – however some generalizations can be made here. Of the four domains mentioned, only land and air-based sensors will likely be of use, as sUAS are too small to be seen, let alone tracked from space and sea-based sensors are unlikely to be utilized outside of warships that happen to be in the area at the time of an sUAS incident.[68] As such, static land-based sensors will be likely be the backbone of any sensor system that is built with the sUAS threat in mind given their persistent data gathering capabilities and low operational cost once built. Beyond land-based capabilities, NORAD should also seek to integrate aerial platforms into current and future air defence and missile warning systems. The goal of these platforms would be to provide additional sensing capabilities where the sensing system has been degraded or destroyed until these can be addressed. This would enable the sensor network to degrade at a slower rate by providing additional redundancy to the sensor network and the potential to provide sensor coverage beyond land-based sensors if required.

The second line of effort that should be undertaken by NORAD is the development of counter sUAS systems for its sensor assets located in Canada and the United States, with an emphasis on those located in Alaska in the near term. By developing this capability, NORAD will be able to mitigate the threat posed by sUAS and ensure that any degradation of its sensor network by hostile actors will be more gradual and costly to effect. While consideration of should be given to both kinetic and non-kinetic solutions, NORAD should place particular emphasis on non-kinetic solutions in this area. One reason for this focus on non-kinetic systems is practicality. Simply put, Canada has not had any land-based air defence capabilities since the Oerlikon Air Defence Anti-Tank System was retired in 2012, and the integration of land-based surface to air missile defences into NORAD would create command and control difficulties as these are army assets in both Canada

and the United States.[69] As a result, this could create bureaucratic frictions between armed services in both countries and, in the Canadian case, a political headache should United States air defence systems be needed to defend the revitalized sensor network – with both taking time and resources away from other important efforts. Additionally, given the cost disparities noted above, currently available kinetic systems are not well suited to counter the sUAS threat – leading to inevitable issues of scalability when engaging more than a handful of sUAS.

The other reason for the emphasis on non-kinetic capabilities is that sUAS are often reliant on communication datalinks when in operation due to many only having limited autonomous capabilities. As such, EW capabilities can mitigate this threat in a variety of ways, including by: warning the remote pilot, jamming the sUAS video, command and control takeover, jamming command and control links, and/or jamming its communications with the global navigation satellite system to which it is connected.[70] Additionally, these EW systems are already available on the commercial market at low cost. As noted in a 2019 United States government global market survey, some 263 non-kinetic systems were available on the global market, with available pricing data indicating that a vast majority of solutions cost less than $1 million USD at the time.[71] Moreover, should the EW capabilities prove insufficient, other non-kinetic solutions such as directed energy weapons and microwave energy weapons could augment this effort with their nearly limitless magazines while also providing more scalability than traditional kinetic solutions.[72] As a result, non-kinetic counter-sUAS systems not only present a lower cost to mitigate the sUAS threat – they can provide this capability faster, and with increased scalability to meet future sUAS threats such as swarms compared to existing kinetic solutions.

Conclusion

The use of sUAS by state and non-state actors poses unique threats to missions across all domains, with the air and missile defence mission-set being no different. In the case of air and missile defence, sUAS, notably offensive payload sUAS, pose a serious threat to the existing air and missile defence structures currently in use due to the pre-existing vulnerabilities of the systems themselves. These vulnerabilities consist of the stovepiping of information sharing capabilities between the various sensing and command nodes within a given AMD system, leading these to become single points of failure. Given their low cost and RCS, sUAS equipped with explosive or electromagnetic warfare payloads have an outsized impact on such AMD systems because they can enter the contested airspace then detect, identify, acquire and prosecute these fail points. Accordingly, this weapons system should be of great concern for any state which operates air and missile defences with these vulnerabilities.

As a binational organization whose principal mission is centered on aerospace defence, NORAD should also be concerned and adapting to mitigate this threat. Currently NORAD is making strides in this direction with the Pathfinder Initiative which is enabling it to breathe new life into aging sensors, allowing it to see threats it would have otherwise missed with the help of AI. Moreover, senior NORAD officials have indicated that they are leaning towards developing a more distributed, networked solution to air and missile defence as part of NORAD's modernization. This will benefit efforts to mitigate the sUAS threat by removing the single points of failure that resulted from the stovepiping of information in the current system. However, while these are good first steps, NORAD needs to develop its own solutions to mitigate the sUAS threat that are cost effective and scalable. In this respect, the development of non-kinetic solutions reliant of EW appears to be a promising

means to provide some level of defence to its northern sensor networks. NORAD should also explore means to supplement current and future sensor networks through the use of air power in order to provide a surging sensor capacity to supplement sensor coverage.

Looking beyond the force protection of NORAD's air and missile defence systems in the Arctic, more thought should be given regarding the use of sUAS by non-state actors to effect attacks against critical infrastructure and human targets. As noted above, these types of attack have been orchestrated by a variety of non-state actors abroad – and given the proliferation of civilian sUAS – the question is not if, but when such attacks will occur in North America. Accordingly, questions regarding NORAD's role in dealing with this threat need to be answered – with the biggest of these being how can it identify, track, and possibly eliminate these threats before reaching their targets? These issues must be addressed to ensure that any additional defences needed, if any, are in place to meet this threat into the future.

[1] James Fergusson, "Canada Must Spend More on Defence or Cede Responsibility to the US: James Fergusson for Inside Policy," *MacDonald-Laurier Institute*, March 29, 2017, https://www.macdonaldlaurier.ca/north-american-defence-in-the-trudeau-trump-era-initial-thoughts-james-fergusson-for-inside-policy/.
[2] Agreement Between the Government of Canada and the Government of the United States of America on the North American Aerospace Defense Command, Canada-United States, April 28, 2006, U.N.T.S. 53359, https://treaties.un.org/Pages/showDetails.aspx?objid=0800000028045ddfc&clang=_en.
[3] Andrea Charron and James Fergusson, "NORAD and the Evolution of North American Defence: Andrea Charron and James Fergusson for Inside Policy," *MacDonald-Laurier Institute*, May 24 2017, https://www.macdonaldlaurier.ca/norad-and-the-evolution-of-north-american-defence-andrea-charron-and-james-fergusson-for-inside-policy/.
[4] Fergusson, "Canada Must Spend More on Defence or Cede Responsibility to the US."
[5] In particular, see Andrea Charron and Jim Fergusson, "NORAD Beyond Modernization," *Centre for Defence and Security Studies*, January 21, 2019, https://umanitoba.ca/centres/cdss/media/NORAD_beyond_modernization_2019.pdf; Andrea Charron and James Fergusson, "From NORAD to NOR[A]D: The Future Evolution of North American Defence Co-operation," *Canadian Global Affairs Institute*, May 2018, https://www.cgai.ca/from_norad_to_nor_a_d_the_future_evolution_of_north_american_defence_co_operation.
[6] See "NORAD Modernization: Report One: Awareness & Sensors," *Conference of Defence Associations Institute*, September 16, 2020, https://cdainstitute.ca/norad-modernization-report-one-awareness-sensors/; "NORAD Modernization: Report Two: Defeat Capabilities," *Conference of Defence Associations Institute*, September 29, 2020, https://cdainstitute.ca/norad-modernization-report-two-defeat-capabilities/; "NORAD Modernization: Report Three: JADC2/JADO," *Conference of Defence Associations Institute*, October 28, 2020, https://cdainstitute.ca/norad-modernization-report-three-jadc2-jado/; Terrence J. O'Shaughnessy and Peter M. Fesler, "Hardening the Shield: A Credible Deterrent & Capable Defense for North America," *Canada Institute* and *Wilson Center*, September 2020, https://www.wilsoncenter.org/publication/hardening-shield-credible-deterrent-capable-defense-north-america.
[7] P. Whitney Lackenbauer, Troy Bouffard, and Nancy Teeple, "The Arctic and North American Defence," *North American and Arctic Defense and Security Network*, December 14, 2020, 3-4, https://www.naadsn.ca/wp-content/uploads/2020/12/Policy-Brief-The-Arctic-and-North-American-Defence.pdf.
[8] "NORAD Modernization: Report One: Awareness & Sensors," *Conference of Defence Associations Institute*;" NORAD Modernization: Report Three: JADC2/JADO," *Conference of Defence Associations Institute*.
[9] For example, see Shaan Shaikh and Wes Rumbaugh, The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense," *Center for Strategic and International Studies*, December 8, 2020, https://www.csis.org/analysis/air-and-missile-war-nagorno-karabakh-lessons-future-strike-and-defense; Jack Watling and Sidharth Kaushal, "The Democratisation of Precision Strike in the Nagorno-Karabakh Conflict," *The Royal United Services Institute*, October 22, 2020, https://rusi.org/commentary/democratisation-precision-strike-nagorno-karabakh-conflict; Thomas Daigle, "Attack on Saudi Oil Facilities Highlights Danger of 'Kamikaze' Drones," *CBC*, September 18, 2019, https://www.cbc.ca/news/technology/tech-drones-saudi-oil-facilities-attacks-1.5287407; Frank Gardner, "Saudi oil Facility Attacks: Race to Restore Supplies," *BBC*, September 20, 2019, https://www.bbc.com/news/world-middle-east-49775849.
[10] United States Department of the Navy, "Close Range UAS," February 21, 2019, https://www.navy.mil/Resources/Fact-Files/Display-FactFiles/Article/2160330/close-range-uas/.
[11] United States Joint Chiefs of Staff, "Joint Air Operations: Joint Publication 3-30," July 25, 2019, III-31, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_30.pdf; United States Department of Defense, "Counter-Small Unmanned Aircraft Systems Strategy," January 7, 2021, 26, https://media.defense.gov/2021/Jan/07/2002561080/-1/-1/0/DEPARTMENT-OF-DEFENSE-COUNTER-SMALL-UNMANNED-AIRCRAFT-SYSTEMS-STRATEGY.pdf.
[12] United States Joint Chiefs of Staff, "DOD Dictionary of Military and Associated Terms," January 2021, 225, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.
[13] Larry Friese, N.R. Jenzen-Jones, and Michael Smallwood, "Emerging Unmanned Threats: The Use of Commercially-Available UAVs by Armed Non-State Actors," *Armament Research Services*, February 18, 2016, 24, https://armamentresearch.com/special-report-no-2-emerging-unmanned-threats/.

[14] For example, see DJI, "DJI FPV Combo," n.d., https://store.dji.com/ca/product/dji-fpv?gclid=CjwKCAjw7J6EBhBDEiwA5UUM2l-ShpiejKQ498afcvIPc-YEF6wjdsbhsOQZWPGtiZSGpiLHTqP-xRoCPc8QAvD_BwE&set_country=CA&vid=101601.
[15] For example, see DJI, "Zenmuse H20 Series," n.d., https://www.dji.com/ca/zenmuse-h20-series?site=brandsite&from=eol_zenmuse-xt; Friese, Jenzen-Jones, and Smallwood, "Emerging Unmanned Threats," 24-25.
[16] See DJI, "Mavic 2," n.d., https://www.dji.com/ca/mavic-2.
[17] See for example, this low cost offering from Snaptain, "SNAPTAIN SP650 1080P HD Camera Beginner Drone," n.d., https://snaptain.com/products/snaptain-sp650-1080p-drone.
[18] See section on Ukraine and the Middle East on pages 38-47, in Friese, Jenzen-Jones, and Smallwood, "Emerging Unmanned Threats."
[19] Insitu, "ScanEagle," n.d., 1-2, https://www.insitu.com/wp-content/uploads/2020/12/ScanEagle_ProductCard_DU120320.pdf.
[20] Friese, Jenzen-Jones, and Smallwood, "Emerging Unmanned Threats." 24-25.
[21] Friese, Jenzen-Jones, and Smallwood, "Emerging Unmanned Threats." 38-39.
[22] Reuters Staff, "Islamic State Drone Kills Two Kurdish Fighters, Wounds Two French Soldiers," *Reuters*, October 11, 2016, https://www.theguardian.com/world/2016/oct/12/exploding-drone-sent-by-isis-allies-kills-and-wounds-troops-in-iraq-report.
[23] Friese, Jenzen-Jones, and Smallwood, "Emerging Unmanned Threats." 29.
[24] For this claim see David Rodman, *Sword and Shield of Zion: The Israel Air Force in the Arab-Israeli Conflict, 1948-2012* (Eastbourne, UK: Sussex Academic Press, 2013), 99, ProQuest Ebook Central. Rodman bases this claim on Richard A. Gabriel, *Operation Peace for Galilee: The Israeli-PLO War in Lebanon* (New York: Hill and Wang, 1984), 99. Dan Gettinger and Arthur Holland Michel, "Loitering Munitions in Focus," *The Center for the Study of Drone*, February 10, 2017, 1, https://dronecenter.bard.edu/loitering-munitions-in-focus/.
[25] Israel Aerospace Industries, "HARPY: Autonomous Weapon for All Weather," n.d., https://www.iai.co.il/p/harpy; Israel Aerospace Industries, "HARPY NG: Anti Radiation Loitering Munition System," n.d., https://www.iai.co.il/drupal/sites/default/files/2019-05/HARPY%20Brochure.pdf; Gettinger and Michel, "Loitering Munitions in Focus," 2.
[26] Israel Aerospace Industries, "HARPY;" Israel Aerospace Industries, "HARPY NG."
[27] The MiG 29 has an RCS of 5m². See Global Security, "F-35 Joint Strike Fighter (JSF) Lightning II," n.d., https://www.globalsecurity.org/military/systems/aircraft/f-35-design.htm.
[28] Israel Aerospace Industries, "HAROP: Loitering Munition System," n.d., https://www.iai.co.il/p/harop.
[29] For more information, see Gettinger and Michel, "Loitering Munitions in Focus," 2-3.
[30] Garrett Reim, "Northrop Pitches UVision Hero Loitering Munition Variant for US Army Future Vertical Lift," *FlightGlobal*, March 10, 2021, https://www.flightglobal.com/military-uavs/northrop-pitches-uvision-hero-loitering-munition-variant-for-us-army-future-vertical-lift/142838.article; Joseph Trevithick, "RAF Tests Swarm Loaded with BriteCloud Electronic Warfare Decoys to Overwhelm Air Defenses," *The Drive*, October 8, 2020, https://www.thedrive.com/the-war-zone/36950/raf-tests-swarm-loaded-with-britecloud-electronic-warfare-decoys-to-overwhelm-air-defenses; A recent article by the RAND Corporation also notes that sUAS could be used for jamming or spoofing Global Positioning System and Global Navigation Satellite System signals, jamming mobile phone signals, and collecting air traffic control signals. For more information, see Bradley Wilson, Shane Tierney, Brendan Toland, Rachel M. Burns, Colby Peyton Steiner, Christopher Scott Adams, Michael Nixon, Raza Khan, Michelle D. Ziegler, Jan Osburg, and Ike Chang, "Small Unmanned Aerial System Adversarial Capabilities," *Rand Corporation*, 2020, 21-25, https://www.rand.org/pubs/research_reports/RR3023.html.
[31] Lockheed Martin PR Newswire, "Lockheed Martin's Shadow Hawk Munition Launched from Shadow UAS For The First Time," *Lockheed Martin*, May 1, 2012, https://news.lockheedmartin.com/2012-05-01-Lockheed-Martins-Shadow-Hawk-Munition-Launched-From-Shadow-UAS-For-The-First-Time.
[32] Textron Systems, "Shadow Tactical Unmanned Aircraft Systems," n.d., https://www.textronsystems.com/products/shadow-tactical-unmanned-aircraft-systems.
[33] Joseph Trevithick, "The Navy Plans to Launch Swarms Of Aerial Drones From Unmanned Submarines And Ships," *The Drive*, March 1, 2021, https://www.thedrive.com/the-war-zone/39535/navy-contract-exposes-plans-to-launch-swarms-of-drones-from-unmanned-boats-and-submarines; Joseph Trevithick, China Conducts Test of Massive Suicide Drone Swarm Launched From a Box on a Truck," *The Drive*, October 14, 2020, https://www.thedrive.com/the-war-zone/37062/china-conducts-test-of-massive-suicide-drone-swarm-launched-from-a-box-on-a-truck.
[34] Kratos Defense, "Kratos XQ-58A Valkyrie Successfully Completes Sixth Flight, Including First Payload Release from Internal Weapons Bay," April 5, 2021, https://ir.kratosdefense.com/news-releases/news-release-details/kratos-xq-58a-valkyrie-successfully-completes-sixth-flight.

[35] Rodman, *Sword and Shield of Zion,* 84.
[36] Rodman, *Sword and Shield of Zion*, 85; Benjamin S. Lambeth, *Air Operation in Israel's War Against Hezbollah: Learning from Lebanon and Getting it Right in Gaza* (Santa Monica: RAND Corporation, 2011), 110-111, https://www.rand.org/pubs/monographs/MG835.html.
[37] Lambeth, *Air Operation in Israel's War Against Hezbollah*, 111.
[38] Tom Karako and Wes Rumbaugh, "Distributed Defense: New Operational Concepts for Air and Missile Defense," *CSIS Missile Defense Project*, January 25, 2018, 10-11, https://missilethreat.csis.org/distributed-defense-new-operational-concepts-air-missile-defense/.
[39] Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, "Report of the Defense Science Board Task Force on Patriot System Performance: Report Summary," January 2005, 2, https://apps.dtic.mil/dtic/tr/fulltext/u2/a435837.pdf.
[40] Ibid.
[41] Karako and Rumbaugh, "Distributed Defense," 10.
[42] Ibid.
[43] Karako and Rumbaugh, "Distributed Defense," 10-15.
[44] See O'Shaughnessy and Fesler, "Hardening the Shield," 8-13.
[45] Peter Layton, "Fifth Generation Air Warfare," *Royal Australian Air Force: Air Power Development Centre*, June 23, 2017, 5, https://airpower.airforce.gov.au/Publications/Working-Paper-43-Fifth-Generation-Air-Warfare.
[46] Karako and Rumbaugh, "Distributed Defense," 18-20.
[47] Karako and Rumbaugh, "Distributed Defense," 21.
[48] United Nations Security Council, *Letter Dated 8 March 2021 from the Panel of Experts on Libya Established Pursuant to Resolution 1973 (2011) Addressed to the President of the Security Council*, March 8, 2021, 17, https://digitallibrary.un.org/record/3905159?ln=en.
[49] Watling and Kaushal, "The Democratisation of Precision Strike in the Nagorno-Karabakh Conflict;" Oryx, "The Fight for Nagorno-Karabakh Documenting Losses on the Sides of Armenia and Azerbaijan," September 27, 2020, https://www.oryxspioenkop.com/2020/09/the-fight-for-nagorno-karabakh.html; Stijn Mitzer and Joost Oliemans, "The Fight for Nagorrno-Karabakh: Documenting Losses on the sides of Armenia and Azerbaijan," September 27, 2021, https://www.oryxspioenkop.com/2020/09/the-fight-for-nagorno-karabakh.html; Stijn Mitzer and Joost Oliemans, "Aftermath: Lessons of the Nagorno-Karabakh War are Paraded through the Streets of Baku," January 26, 2021, https://www.oryxspioenkop.com/2021/01/aftermath-lessons-of-nagorno-karabakh.html.
[50] Daigle, "Attack on Saudi Oil Facilities Highlights Danger of 'Kamikaze' Drones."
[51] Wierzbanowski, "Gremlins," *Defense Advanced Research Projects Agency*, n.d., https://www.darpa.mil/program/gremlins#:~:text=The%20Gremlins%20program%20plans%20to%20explore%20numerous%20technical,digital%20flight%20control%2C%20relative%20navigation%20and%20station%20keeping; Naturally, forward deploying loitering munitions at sea in the Arctic would be dependent on ice conditions, and would therefore be more difficult. However, it is still a possibility to consider nonetheless. See Ryan White, "US Navy Plans to Buy Submarine-Launched Blackwing UAVs," March 19, 2021, https://navalpost.com/us-navy-submarine-launched-uav-aerovironment-blackwing/.
[52] O'Shaughnessy and Fesler, "Hardening the Shield," 8-9.
[53] David Hambling, "Russia Uses 'Swarm of Drones' in Military Exercise for the First Time," *Forbes*, September 24, 2020, https://www.forbes.com/sites/davidhambling/2020/09/24/russia-uses-swarm-of-drones-in-military-exercise-for-the-first-time/?sh=4a136f1f4771. This is also evidenced by the current capabilities publicly advertised by Russian UAS manufacturers such as ZALA Aero Group who's UAS are both limited in payload and range.
[54] The Russia Studies Program, "Artificial Intelligence in Russia: Issue 22," March 12, 2021, 7, https://www.cna.org/CNA_files/PDF/DOP-2021-U-029392-Final.pdf; Roger McDermott, "Russian UAV Technology and Loitering Munitions," May 5, 2021, https://jamestown.org/program/russian-uav-technology-and-loitering-munitions/; Samuel Bendett, "Russia Plans More Arctic UAVs," *Defense One*, February 20, 2019, https://www.defenseone.com/ideas/2019/02/russia-plans-more-arctic-uavs/154998/.
[55] Gary Martinic, "Swarming, Expendable, Unmanned Aerial Vehicles as a Warfighting Capability," *Canadian Military Journal* 20, no. 4 (2020): 44, http://www.journal.forces.gc.ca/vol20/no4/page43-eng.asp.
[56] Amanda Macias, "Russia is Luring International Arms Buyers with a Missile System that Costs Much Less than Models Made by American Companies," *CNBC*, November 19, 2018, https://www.cnbc.com/2018/11/19/russia-lures-buyers-as-s-400-missile-system-costs-less-than-us-models.html#:~:text=Russia%E2%80%99s%20S-400%2C%20a%20mobile%20long-range%20surface-to-

air%20missile%20system%2C,with%20first-hand%20knowledge%20of%20a%20U.S.%20intelligence%20assessment; Derek Hawkins, "A U.S. 'Ally' Fired a $3 Million Patriot Missile at a $200 Drone. Spoiler: The Missile Won.," *The Washington Post*, March 17, 2017, https://www.washingtonpost.com/news/morning-mix/wp/2017/03/17/a-u-s-ally-fired-a-3-million-patriot-missile-at-a-200-drone-spoiler-the-missile-won/.

[57] "NORAD Modernization: Report Two: Defeat Capabilities," *Conference of Defence Associations Institute*.

[58] Derek Hawkins, "A U.S. 'Ally' Fired a $3 Million Patriot Missile at a $200 Drone. Spoiler: The Missile Won.;" Saudi Arabia is perhaps the best example of a state pursuing this approach to meet its current needs, see Joseph Trevithick, "Watch A Saudi F-15 Fighter Swoop In Low To Blast A Houthi Rebel Drone Out Of The Sky," *The Drive*, March 30, 2021, https://www.thedrive.com/the-war-zone/39992/watch-a-saudi-f-15-fighter-swoop-in-low-to-blast-a-houthi-rebel-drone-out-of-the-sky.

[59] United States Senate Armed Services Committee, *Statement of General Glen D. Vanherck, United States Air Force Commander United States Northern Command and North American Aerospace Defense Command, by General Glen D. Vanherck, which was read before the Subcommittee on Strategic Forces,* June 9, 2021, 11, https://www.armed-services.senate.gov/hearings/missile-defense-strategy-policies-and-programs-in-review-of-the-defense-authorization-request-for-fiscal-year-2022-and-the-future-years-defense-program.

[60] Nathan Strout, "NORAD is Using Artificial Intelligence to See the Threats it Used to Miss," *C4ISR*, March 1, 2021, https://www.c4isrnet.com/artificial-intelligence/2021/03/01/norad-is-using-artificial-intelligence-to-see-the-threats-it-used-to-miss/.

[61] O'Shaughnessy and Fesler, "Hardening the Shield," 11-12; Strout, "NORAD is Using Artificial Intelligence to See the Threats it Used to Miss."

[62] See Nunatsiaq News, "Fire Destroys North Warning System Radar Station," *Nunatsiaq News*, January 14, 2000, https://nunatsiaq.com/stories/article/fire_destroys_north_warning_system_radar_station/; James Fergusson, "Missed Opportunities: Why Canada's North Warning System is Overdue for an Overhaul," *MacDonald-Laurier Institute*, January 14, 2020, 2, https://www.macdonaldlaurier.ca/canadas-north-warning-system-needs-overhaul-new-mli-commentary/.

[63] "NORAD Modernization: Report Two: Defeat Capabilities," *Conference of Defence Associations Institute*.

[64] O'Shaughnessy and Fesler, "Hardening the Shield," 10.

[65] Wilson et al., "Small Unmanned Aerial System Adversarial Capabilities," 111.

[66] Ibid.

[67] Ibid.

[68] For example, Canada's RADARSAT-2 is only capable of one-by-three-meter resolution imaging on spotlight mode. Also, RADARSAT-2 can only orbit over the high Arctic up to four times a day due to its orbit, thereby limiting its usefulness as a sensor even if it was capable of detecting sUAS to begin with. For more information, see Government of Canada, "What is RADARSAT-2," January 8, 2021, https://www.asc-csa.gc.ca/eng/satellites/radarsat2/what-is-radarsat2.asp; Government of Canada, "RADARSAT Satellites: Technical Comparison," January 12, 2021, https://www.asc-csa.gc.ca/eng/satellites/radarsat/technical-features/radarsat-comparison.asp.

[69] Charron and Fergusson, "NORAD Beyond Modernization," 41; Murray Brewster, "Canada Needs Updated Anti-Aircraft Systems for the Modern Battlefield, Says Army Commander," *CBC*, December 18, 2019, https://www.cbc.ca/news/politics/anti-aircraft-canadian-forces-1.5399461.

[70] Scott Brooks, Carol Jacobus, Camron Kouhestani, John Stikar, and Erik Faye, "Counter-Unmanned Aircraft Systems Market Survey," *Sandia National Laboratories*, March 1, 2019, 41, DOI: https://doi.org/10.2172/1761916.

[71] Brooks et al., "Counter-Unmanned Aircraft Systems Market Survey," 29-31.

[72] This scalability can be seen in Epirus' Leonidas, for example, which the company claims can eliminate individual and swarms of sUAS. See Epirus Inc., "Leonidas," n.d., https://www.epirusinc.com/products.