National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

Defending Against Uninhabited Aerial Vehicles in the Maritime Environment

Lieutenant-Commander Richard Crowder

JCSP 48

Service Paper

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 48

Étude Militaire

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 48 – PCEMI 48
2021 – 2022

Service Paper – Étude militaire

Defending Against Uninhabited Aerial Vehicles in the Maritime Environment

Lieutenant-Commander Richard Crowder

DEFENDING AGAINST UNINHABITED AERIAL VEHICLES IN THE MARITIME ENVIRONMENT

Aim

1. This paper discusses how the Royal Canadian Navy (RCN) should address the threat of unmanned aerial vehicles (UAVs) in the maritime environment. This includes what challenges the RCN faces in properly defending against UAVs, how these challenges can be mitigated, and what action might be required of the RCN and the Canadian Armed Force (CAF) to address these threats in the future. Owing to the significant differences between the above and underwater battlespace, the focus of this paper is on airborne threats only. There are recommendations included for further investigation.

Introduction

2. As Artificial Intelligence (AI) proliferates across both civilian and military industrial domains, the previously unimaginable becomes normal, and the boundaries of what new capabilities AI might bring are expanded. There is a tendency to ascribe special capabilities to AI owing to an aura of incomprehensibility, but AI is simply a computer performing a function that previously would have been accomplished by a human operator.[1] The Combat Management System installed in the Halifax-class is an example of this, whereby analysis of sensors and weapon employment recommendations that were formerly made by human operators can now be reliably conduct by software, with the reliability and repeatability of the system reducing the possibility of human error. The operator chooses how involved they remain within the cycle. This enables faster and more accurate responses in self defense, especially in the discipline of anti-ship missile defense. Anti-ship missiles themselves are an AI system, using human input parameters to locate a specified target and attempt to penetrate its defense. While most Naval Warfare specialists would not look at these and think to label it artificial intelligence, imagine what their predecessors in a corvette might have said upon seeing a computer replace paper plots, gunnery calculators, and hand-set fuzes. It has already existed in the RCN for some time, and in the example above, is specifically designed to counter threats that are likewise controlled by AI. Understanding AI as simply an automated decision-making process is important to framing discussion how to counter AI, as it is imperative to recognize that there is no magic involved, simply a computer, however advanced. This does not mean that AI enabled weapons are somehow less threatening, but serves to frame the discussion. Military technologies have long seesawed in this relationship between disruptive new threats and resulting developments that can effectively defend against them.[2] The UAV threat is simply one of the latest.

3. The concurrent development of unmanned vehicles and the latest generation of AI has combined to present new threats to conventional forces, with reports of swarm of small drone attacks against Russian forces in Syria, bombarding Saudi oil production facilities, and drones

[1] Haenlein, Michael, and Andreas Kaplan. "A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence." *California Management Review 61, no. 4* (August 2019): 5–14. 5.
[2] Hammes, T.X. "The Future of Warfare: Small, Many, Smart vs. Few & Exquisite?" *War on the Rocks*, August 7, 2015. https://warontherocks.com/2014/07/the-future-of-warfare-small-many-smart-vs-few-exquisite

stalking US Navy warships[3] highlighting the challenge posed by unmanned aerial systems. They are difficult to detect and target using traditional sensors, or the human eye for that matter; and difficult to defeat using conventional weapons systems.[4] Even when it is possible to destroy such UAVs using guns or missiles, it can still be something of a victory for the attacking force, as our defensive systems are generally significantly more expensive to deploy than the threats themselves. [5] This is especially true in the maritime environment, where excepting small arms, supply of expensive defensive armaments is limited, especially those designed to counter aircraft and anti-ship missiles. Reducing our available armament in defending against nuisance attacks by UAVs would certainly be to the advantage of an adversary, especially if they can do so at lower cost and without risking their own lives.[6] While the majority of known attacks by UAVs against conventional forces have been by non-state actors, great powers are also investing in these capabilities, and the Chinese government has sought to create legal space for their use within the laws of armed conflict.[7] This threat is not confined to conflicts with extremist organizations or proxy forces.

4. So, what do navies do to defend against these essentially asymmetric threats? We have no further to look than the allied navy response to the asymmetric threat following the bombing of the USS *Cole* in 2001. Navies developed specific doctrine to address these threats, procured or modified defensive systems to specifically counter them, and created task-tailored organizations to respond to asymmetric surface threats. In the RCN, these are the Force Protection organization (FP Org) and more recently the Naval Security Team (NST).[8] These teams complement the normal fighting organization of ships and serve to mitigate the asymmetric threat when conventional defense would be marginal or inappropriate. This pattern of response remains valid and should be implemented to counter the threat of UAVs.

Discussion

5. The threat UAVs present to ships is not homogenous, as there are multiple varieties of platform which can be employed against ships, with varying sizes, payloads, ranges, and control systems. Accordingly, the response needs to be flexible enough to match the threat, while avoiding seams in defense by ensuring that there is overlap between different responses. This is achieved by having complimentary organizations that respond to threats, each with some degree of capability in countering the principal threat that the others are oriented towards. In traditional counter surface Force Protection, this is achieved by the overlap of the Above Water Warfare (AWW) and FP Orgs, combining the large caliber main armament and Close in Weapon System with the small arms of the FP Org to present a flexible response against small boat, littoral, or

---

[3] Ceotti, Marc, Kehoe, Adam. *"Navy Destroyer Deployed Counter-Drone Electronic Warfare System During 2019 Mystery Swarm Incident*." www.thedrive.com. 14 Jan 2022.
[4] Safi, Michael and Julian Borger. *"How did Attack Breach Saudi Defences and what Will Happen Next?"* Guardian News & Media Limited.
[5] Hambling, David. "Swarm of Drones Attacks Airbase." *New Scientist 237, no. 3161* (January 20, 2018): 12.
[6] Wills, C. *Unmanned Combat Air Systems in Future Warfare: Gaining Control of the Air.* London: Palgrave Macmillan UK, 2015. 29.
[7] Ryan Fedasiuk, Jennifer Melot, and Ben Murphy *"Harnessed Lightning."* Center for Security and Emerging Technology, October 2021. 43.
[8] Canada. Department of National Defence. CFCD 129. RCN Readiness and Sustainment Policy. Ottawa: DND Canada, 2018. Annex A to Chapter 4.

shore-based threats. The AWW team is ready to provide stand-off engagement, and if the risk of collateral damage is too great to use heavier weapons or the probably of a kill falls as the range of the target becomes too close, the FP Org is prepared to apply small arms fire using both crew served and individual weapons from appropriate positions. This same principle can be applied defense against asymmetric airborne threats. The AWW Organisation will use the same procedures and systems to detect, target, and destroy threats, while handing over those targets that cannot be engaged to the FP Org for defense.

6. The key difference for the FP Org will be the tools they employ to defend the ship, as employing small arms against UAVs is difficult at best owing to the challenge in visually acquiring these targets and accurately firing weapons, and next to impossible in the context of multiple manoeuvring targets.[9] HMCS *Calgary* and *Regina* conducted anti-UAV testing using C2 .50 calibre heavy machine guns mounted in the Naval Remote Weapon System (Mini-Typhoon) during Canadian Fleet Pacific Task Group Exercise 21-02 in June 2021.[10] Even with cueing from the AWW organization, the operators were challenged to successfully detect, track, and engage relatively large Vindicator drones, owing to the limitations of the system in solving ballistic problems. This same poor result was repeated when operators attempted to conduct the engagements by manually operating the weapons at the mounts instead of using the remote-control system. Those UAVs were typical of most-state owned armed UAVs, and easily engageable with conventional air defense systems, but it provides useful context for the following anecdote. HMCS *Calgary* also participated in anti-UAV testing with USS *Gridley* in February 2019, where even smaller target profiles were presented, typical of commercial off the shelf UAVs that have been modified for hostilities in the Middle East.[11] Neither ship was able to detect these UAVs unalerted, and even when alerted and cued to the threat axis, were only able to establish intermittent radar contact, in spite of employing specific radar settings intended to maximize the probability of detecting UAVs. While these settings are sufficient for traditional large military UAVs, the use of smaller commercial UAVS rendered detection next to impossible. Their small size presents a minuscule radar cross section, they generate little infrared signature aside from ambient differences, and their ability to fly slower than typical air threats presents a minimal doppler effect for radars to track. Had these targets been hostile, neither ship would have been able to defend itself using the systems at hand. The present means of employing force to counter this threat are not fit for purpose.

7. The US Navy is seized with the potential threat of UAVs against their ships and has invested in regular testing to evaluate potential off the shelf and bespoke systems designed to counter these asymmetric threats. They have begun deploying these in their Fleets (as have the other US services) on an interim basis, while continuing to refine these systems in research and

---

[9] Stoica, Andrei-Alexandru. *"Legal Status of Anti-Drone Systems Under International Law."* Challenges of the Knowledge Society (2019): 795.

[10] The author was the Assistant Test Director for this exercise. Significant effort was made to create plausible engagements for the FP Org, ranging from alerted engagements where the operators did not know the axis of threat to fully disclosed engagements where the operators knew the exact flight profile of the target.

[11] COTS UAVs were launched from San Clemente Island as well as from range vessels simulating adversaries. The cueing provided was directly from control stations, and thus very accurate. This exercise also saw the US Navy testing dedicated UAV detection and defensive systems, alluded to in the article at Footnote 2.

development.[12] Their concept of employment is not dissimilar from the RCN FP Org, where a small team is provided specialized equipment and training to complement the regular fighting organization in close in air defence. The current iteration consists of a human carried all in one system that detects the control signals of remotely controlled UAVs, localizes the source, and enables the operator to choose to jam the control signal with radio frequency energy. These systems can disrupt the command and control of remotely piloted UAVs, but not UAVs operating autonomously. The same principle can be applied however in disrupting swarms, by either disrupting or hijacking the control signal between UAVS.[13] These defensive systems are not exquisite military capabilities either, as the civilian aviation industry is equally concerned with interdiction of UAVs that trespass into airports or airways. This capability is advancing rapidly, driven by moth military and civilian demand, and is becoming widely available. They are designed to be simple to operate, with minimal training. But this still leaves the question of how to defend against truly autonomous UAVs that require no operator to acquire and engage a target. For these, a more active approach is required.

8. We have already discussed the disproportionate cost of employing regular air defence weapons against UAVs, which has drawn public criticism in past incidents of UAV defense.[14] This might be reasonable against larger, potentially more destructive platforms, but if pressed into service against smaller, COTS-type weapons, our traditional systems are now both not cost-effective and less effective. Specialized kinetic systems are required for defense, but thankfully these also exist already, and continue to be refined. These include friendly UAVs equipped with nets that are capable of capturing or downing targets. While this concept is dynamic and able to provide a degree of standoff defense, it is also limited by its inability to counter a swarm of UAVs. More appropriate for a maritime platform are static systems such as the Israeli "Drone Dome," that in addition having the capability of disrupting or jamming, is armed with directed energy weapons that are capable of conducting a hard kill against small UAVs.[15] Again, much like the non-kinetic systems that can be used to disrupt remotely piloted UAVS, these systems are readily available, require minimal training, making them suitable for employment by the AWW or FP Organizations in RCN platforms. One significant challenge in employing these systems will mirror that of other force protection doctrine, the balance of seeking to avoid collateral damage against the right and requirement to exercise self defense. Most states have strict regulations against the use of jamming radio frequencies for good reason, as the same effect that is intended

Conclusion

9. While the spectre of swarms of AI enabled drones massing against ships seems like a scenario from science fiction, it is a plausible reality now, given the advancement of UAV technology, the proliferation of low-cost platforms, and the interest of adversary militaries. This

---

[12] US Navy. Capt Malatesta, PMS 408 Briefing. *"Sea Air Space 2021."* https://www.navsea.navy.mil/Portals/103/Documents/Exhibits/SAS2021/SAS2021-Expeditionary%20Missions.pdf, accessed 23 Jan 22.
[13] Park, Seongjoon, Hyeong Tae Kim, Sangmin Lee, Hyeontae Joo, and Hwangnam Kim. *"Survey on Anti-Drone Systems: Components, Designs, and Challenges."* IEEE Access 9, (2021): 42635-42659.
[14] Stoica, Andrei-Alexandru. *"Legal Status of Anti-Drone Systems Under International Law."* Challenges of the Knowledge Society (2019): 795.
[15] *Ibid*., 797.

does not mean that the RCN is suddenly without the means to defend itself however, as it already has doctrine and procedures which can be easily adapted to counter the UAV threat. What is missing from their capability is now simply a matter of equipment, which already exists, to counter both remotely piloted and autonomous small UAVs. These systems are both commercially available and available through our partners and allies. They should be integrated in RCN Force Protection doctrine and training without delay, while continuing to develop permanent solutions that cross seamlessly between traditional air warfare and force protection.

Recommendations

10. CFMWC and DRDC should evaluate currently available anti drone systems, such as the USN DRAKE man portable system to counter remotely piloted UAVs, and the Drone Dome system by Rafael, for hard kill of remotely piloted and autonomous UAVs. These tests should evaluate their ability to operate in environments typical of ships alongside, in littoral areas, and on the high seas, and against both military and commercially available UAVs. Other L1 organizations may already be engaged in similar evaluation and the RCN should seek to avoid duplicating effort where possible, and instead leverage their experience to expedite adoption of this capability.

11. If such systems are deemed to be safe, suitable, and fit for purpose, they should be procured on a mission fit basis for RCN ships being Force Employed in areas of known adversary UAV activity, such as the Black Sea, Persian Gulf, and South and East China Seas. Individual training will be required for the designated operators, and readiness training will need to include the integration of these capabilities into the AWW and FP Orgs, with a particular focus on criteria and process for transition from AWW to FP Org.

12. The RCN should engage the Naval Security Team to support testing and development, to develop their corporate knowledge of anti-UAV doctrine, procedures, and systems in both alongside and underway force protection. This could provide additional meaningful opportunities and demand for the NST in both Force Generation and Force Employment.

13. Trinity MOSIC should include assessments on UAV capability and activity by both state and non-state actors in preparing port Threat Assessments and pre-deployment briefings for RCN ships.

BIBLIOGRAPHY

Canada. Department of National Defence. CFCD 129. *RCN Readiness and Sustainment Policy.* Ottawa: DND Canada, 2018. Annex A to Chapter 4.

Ceotti, Marc, and Adam Kehoe. *Navy Destroyer Deployed Counter-Drone Electronic Warfare System During 2019 Mystery Swarm Incident*. www.thedrive.com. 14 Jan 2022.

Haenlein, Michael, and Andreas Kaplan. "A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence." California Management Review 61, no. 4 (August 2019): 5–14.

Hambling, David. "Swarm of Drones Attacks Airbase." New Scientist 237, no. 3161 (January 20, 2018).

Hammes, T.X. "The Future of Warfare: Small, Many, Smart vs. Few & Exquisite?" War on the Rocks, August 7, 2015. https://warontherocks.com/2014/07/the-future-of-warfare-small-many-smart-vs-few-exquisite

Park, Seongjoon, Hyeong Tae Kim, Sangmin Lee, Hyeontae Joo, and Hwangnam Kim. *"Survey on Anti-Drone Systems: Components, Designs, and Challenges."* IEEE Access 9, (2021): 42635-42659.

Ryan Fedasiuk, Jennifer Melot, and Ben Murphy *"Harnessed Lightning."* Center for Security and Emerging Technology, October 2021.

Safi, Michael and Julian Borger. "How did Attack Breach Saudi Defences and what Will Happen Next?" Guardian News & Media Limited.

Stoica, Andrei-Alexandru. *"Legal Status of Anti-Drone Systems Under International Law."* Challenges of the Knowledge Society (2019): 795-802.

US Navy. Capt Malatesta, PMS 408 Briefing. *"Sea Air Space 2021."* https://www.navsea.navy.mil/Portals/103/Documents/Exhibits/SAS2021/SAS2021-Expeditionary%20Missions.pdf, accessed 23 Jan 22.

Wills, C. "*Unmanned Combat Air Systems in Future Warfare: Gaining Control of the Air."* London: Palgrave Macmillan UK, 2015.