National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

DETECTING AND DEFEATING THE SMALL UNMANNED AERIAL SYSTEMS THREAT

Major Benjamin Chapman

JCSP 50	PCEMI n° 50
Service Paper	**Étude militaire**

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.

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 50 - PCEMI n° 50
2023 - 2024

Service Paper – Étude militaire

DETECTING AND DEFEATING THE SMALL UNMANNED AERIAL SYSTEMS THREAT

Major Benjamin Chapman

"This paper was written by a candidate attending the Canadian Forces College in fulfilment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defence."

« La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de difuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale. »

DETECTING AND DEFEATING THE SMALL UNMANNED AERIAL SYSTEMS THREAT

AIM

1. With the continued global proliferation of small unmanned aerial systems (sUAS) for commercial and military purposes, the use of these systems in armed conflicts around the world has been growing rapidly. The threats posed by sUAS can range widely from nuisance use in vicinity of Canadian Armed Forces (CAF) infrastructure, to serious threats from enemy surveillance and direct attacks by weapon systems mounted to the sUAS. Current conflicts, including the war in Ukraine, have seen sUAS attacks occurring regularly with platforms becoming increasingly accurate, lethal, and difficult to defeat. The aim of this service paper is to propose recommendations for the procurement of counter sUAS capabilities to enhance the protection of CAF personnel, equipment, and infrastructure both domestically and on deployed operations.

INTRODUCTION

2. The rate of technological change within the commercial and military sUAS space has made the detection and defeat of these aerial threats a challenge. While no detection system is perfect, the multitude of sUAS types available provide an adversary with the capacity to adjust their tactics or equipment to evade certain detection systems. This ability to quickly adjust tactics and modify in-service sUAS has been an essential element that has allowed Ukrainian forces to keep ahead of Russian counter sUAS efforts.[1] As a result of the speed at which the sUAS threat can shift, it is important that counter sUAS capabilities are also developed with flexibility in mind. Detection is challenging with emergent sUAS capable of leveraging different means of control including radio-control (RC) across a wide range of frequency bands, satellite signal control through GPS or GLONASS, and control through the use of cellular network signals.[2] Defeat can also be challenging with modern sUAS reaching speeds in excess of 72 km/hr and capable of conducting night operations when equipped with advanced optics.[3] At the same time, payload is increasing with purpose built military sUAS capable of carrying up to eight 60mm mortar rounds and loitering above a target for over 20 minutes.[4] With rapidly changing technology, relying on a single method to detect or defeat sUAS threats will not be effective, and a scalable multi-sensor system would offer greater versatility to the CAF for domestic and deployed use.

[1] Fareed Zakaria. “Interview With President Volodymyr Zelenskyy and Mykhailo Fedorov About Ukraine’s Army Of Drones and Ukraine’s Children Of War.” Fareed Zakaria Global Public Square, aired (2023).

[2] Bradley Wilson, Shane Tierney, Brendan Toland, Rachel M. Burns, Colby Peyton Steiner, Christopher Scott Adams, Michael Nixon, et al. “Small Unmanned Aerial System Adversary Capabilities.” *Policy File*. RAND Corporation, (2020). 39.

[3] Travis Cline and J. Dietz. “Agent Based Modeling for Low-Cost Counter UAS Protocol in Prisons.” *International Journal of Aviation, Aeronautics, and Aerospace*, vol 7, issue 2, article 2, (2020). 8.

[4] Josef Danczuk. “Bayraktars and Grenade-Dropping Quadcopters: How Ukraine and Nagorno-Karabakh Highlight Present Aid and Missile Defense Shortcomings and the Necessity of Unmanned Aircraft Systems.” *The Military Review: The Professional Journal of the US Army*, (2023). 27.

3. This service paper will first define what is considered a sUAS and will then provide recommendations on counter sUAS capabilities including systems for the detection and tracking of sUAS, as well as systems for the defeat of sUAS using kinetic and non-kinetic interdiction methods.

DISCUSSION

Definition

4. As there are now several categories of UAS it is important to define what a sUAS is, and for this service paper the NATO classification tables will be used. By the NATO definition, a sUAS falls into the category of a Class I UAS. Class I UAS have weights of less that 150 kg, fly at altitudes less than 1,700 meters above ground level, and have normal mission radiuses of less than 50 km.[5] The Class I UAS definition does not further differentiate sUAS by their method of control, nor does it separate commercial models from those made specifically for military purposes. Due to the size and operating altitudes of Class II and III UAS, the methods to detect and defeat them are more consistent with traditional forms of air defense, and they will not be considered in this discussion.

Detection and tracking of sUAS

5. The first critical step in defeating sUAS is identifying that there is an existing threat in the area. While this may seem like a relatively simple matter in theory, in practice it can be both difficult to detect an adversarial sUAS, and even more difficult to detect one fast enough to deploy effective counter measures against it.[6] Numerous reasons exist for the difficulty in detecting sUAS including the wide range of available frequencies for control, the ability to set pre-programmed flight paths,[7] their small size, their ability to operate a low speeds and altitudes, and the incentive for commercial and military manufacturers to create quieter products.

6. As state and non-state actors will continue to endeavour to make the detection and defeat of sUAS more challenging, it is of critical importance that a multi-sensor detection capability be procured to ensure that detection can be accomplished in a variety of ways. While multi-sensor arrays create additional challenges due to their complexity and size, leveraging multiple sensor inputs will provide a higher likelihood that sUAS threats can be detected effectively. Once detected, a multi-sensors system will also allow for better tracking of the sUAS within the area interest.[8]

7. Passive radio frequency (RF) detectors should be considered an important element of a detection system as they are capable of detecting the means of control of a large number of

[5] Georgia Lykou, Dimitrios Moustakas, and Dimitris Gritzalis. "Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies." *Sensors (Basel, Switzerland)* 20, no. 12 (2020). 3.

[6] Travis Cline and J. Dietz. "Agent Based Modeling for Low-Cost Counter UAS Protocol in Prisons." 11.

[7] Bradley Wilson, et al. "Unmanned Aerial System Adversary Capabilities." 106 – 107.

[8] US Department of Defence. "Army Techniques Publication No. 3-01.81. Counter-Unmanned Aircraft Systems (C-UAS)." Department of the Army, Washington DC. (2023). 3-8.

available sUAS, and have the additional benefit of being a non-emitting sensor.[9] Some sUAS designed specifically for military purposes may not present a RF signature depending on their means of control, while others may be identifiable through passive RF detectors.[10] As such, while likely effective against commercial sUAS, passive RF detection could fall short against specific threats in a deployed context. Further, while a single detector of this type can determine the bearing to a potential threat, multiple dispersed RF detectors are needed to accurately determine the position and elevation of the sUAS.[11] This creates a requirement to receive and process inputs from an array of RF detectors in order to ensure accuracy. RF detection can be made further problematic in areas with high ambient RF saturation, such as urban environments, and RF detectors have also been shown to have difficulty when trying to identify multiple sUAS at a time.[12]

8. The additional sensors that should be employed in a comprehensive detection system include visual sensors such as electro-optic (EO) and infrared (IR), acoustic sensors, and radar sensors including doppler radar. Like passive RF sensors, each of these sensor types have specific strengths and weaknesses. As a result, relying on only one of them will not provide sufficient protection against the full range of potential threats. A layered multi-sensor approach will provide higher assurance that a sUAS will be detected, and once a detection is made, will allow the higher resolution sensors to track the threat.

9. Visual sensors are highly accurate when detecting objects at close range but are limited by numerous factors including line of sight, direction the sensor is observing, and obscurants such as smoke and fog.[13] Visual sensors can also misidentify sUAS and require a degree of machine learning to ensure that the sensors can effectively differentiate sUAS from other objects such as birds. While machine learning processes have been successful in ensuring a visual sensor can identify an sUAS the majority of the time, false positives and false negatives can still occur.[14]

10. Acoustic sensors have proven successful in the detection of sUAS but also have several limitations. Acoustic detection can be undermined by background noise or by terrain that causes a disruption in the propagation of sound waves, ultimately limiting their detection range and necessitating multiple microphone arrays.[15] Acoustic detection is also being made more difficult as a result of the desire from both the military and civilian sectors to silence their sUAS.[16] Like

[9] Georgia Lykou et al. "Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies." 9.

[10] Lacher, Andrew, Jonathan Baron, Jonathan Rotner, and Michael Balazs. "Small Unmanned Aircraft: Characterizing the Threat." The MITRE Corporation, (2019). 5-6.

[11] Bradley Wilson, et al. "Unmanned Aerial System Adversary Capabilities." 106.

[12] Georgia Lykou et al. "Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies." 9.

[13] Stamatios Samaras, Eleni Diamantidou, Dimitrios Ataloglou, Nikos Sakellariou, Anastasios Vafeiadis, Vasilis Magoulianitis, Antonios Lalas, et al. "Deep Learning on Multi Sensor Data for Counter UAV Applications-A Systematic Review." *Sensors (Basel, Switzerland)* 19, no. 22 (2019). 25.

[14] E. Çetin, C. Barrado, and E. Pastor. "Improving Real-Time Drone Detection for Counter-Drone Systems." *Aeronautical Journal* 125, no. 1292 (2021). 1875-76.

[15] Stamatios Samaras, et al. "Deep Learning on Multi Sensor Data for Counter UAV Applications-A Systematic Review." 25.

[16] Bradley Wilson, et al. "Unmanned Aerial System Adversary Capabilities." 107-109.

visual sensors, acoustic sensors need some degree of machine learning to know what they are listening for, and can miss sounds that they have not been trained to identify as a threat.[17]
11. Finally, radar and doppler-radar identify sUAS by emitting electromagnetic (EM) radiation in the form of waves and detecting and analysing the returning wave patterns.[18] These sensors are generally less impacted by weather conditions than visual sensors, but due to the small size and low flying nature of sUAS, radar systems can have difficulty detecting the cross-sectional area of sUAS.[19] While radar effectiveness decreases over long distances or when there are obstacles between the sensor and target, radar remains an accurate method of determining the direction and range to a target. Radar, unlike other sensors, has the draw back of emitting detectable energy, and while those emissions may not be of concern when used domestically or in a non-threat environment, they could be detected and targeted by an adversary in a contested environment.

12. The use of a multi-sensor system will allow for the fusion of several sensor inputs to more successfully detect threats by avoiding the weaknesses of a single sensor, and will enable multiple sensors to track the detected sUAS.[20] Additionally, while a single multi-sensor array may be suitable for protecting a small area, larger areas such as bases and airfields may be insufficiently protected depending on the nature of the terrain. To overcome dead spots in sensor coverage, several multi-sensor arrays may be necessary to provide detection and tracking capabilities over these larger areas. It is therefore critical that detection systems not only leverage different types of sensors but should also be scalable to receive inputs from multiple sensor arrays positioned over a dispersed area. The multi-sensor nature of the detection system will enhance coverage while ensuring that a known weakness of an individual sensor can not be exploited. Scalability will ensure that larger areas can be protected through a layering of sensors and will allow for sensors to be added or removed in different environments or to counter specific threats.

Defeating the sUAS threat

13. Like detection, consistently defeating sUAS is challenging and should not rely on a single method to achieve the defeat of the threat. Further, due to the speed of modern sUAS, automated defeat systems linked to the detection and tracking system would provide a higher likelihood of destroying individual or multiple sUAS threats. With sUAS capable of speeds in excess of 72 km/hr, only a small window of time is available to identify the threat and employ an effective counter measure against it. Without some degree of automation in the process, the time required to effectively respond to a threat may be too short. Human initiated interdiction devices such as the “Drone Buster” should be made available for use but will not be effective in all situations.[21]

[17] Stamatios Samaras, et al. “Deep Learning on Multi Sensor Data for Counter UAV Applications-A Systematic Review.” 23.

[18] Bradley Wilson, et al. “Unmanned Aerial System Adversary Capabilities.” 88.

[19] Abdulhadi Shoufan, and Ernesto Damiani. “Contingency Clarification Protocols for Reliable Counter-Drone Operation.” *IEEE Transactions on Aerospace and Electronic Systems* 59, no. 6 (2023). 8946.

[20] Juan A. Besada, Ivan Campaña, David Carramiñana, Luca Bergesio, and Gonzalo de Miguel. “Review and Simulation of Counter-UAS Sensors for Unmanned Traffic Management.” *Sensors* (Basel, Switzerland) 22, no. 1 (2021). 11.

[21] US Department of Defence. “Army Techniques Publication No. 3-01.81. Counter-Unmanned Aircraft Systems (C-UAS).” Department of the Army, Washington DC. (2023). B-2.

Human operated devices require line of sight, are difficult to use accurately at night, and could be overwhelmed by large numbers of sUAS in a single area. As such, an automated defeat system would offer superior protection over one that requires significant human interaction.

14. Of the integrated counter sUAS systems that can be employed once a threat has been identified, systems that interrupt the ability of the operator to control the sUAS have proven effective. These systems can include stationary or portable RF disruptors as well as UAS spoofing devices. The RF disruptors, also referred to as jammers, can be integrated with the detection systems and are capable of defeating RF controlled sUAS including those controlled via satellite and cellular signals.[22] Unfortunately, there may be circumstances where the use of RF disruptors could be problematic, such as near airfields and sensitive electronic equipment.[23] As a result, specific policies would be needed to ensure that RF disruptors are permissible for use in an area before they are employed. Spoofing devices are similar to RF disruptors, in that they are used to disrupt the means of control of sUAS, but spoofing devices have the additional capability of taking control of the sUAS and can force it to land in a specified area.[24] The use of RF disruption and spoofing should be incorporated as part of the soft kill capability in a comprehensive sUAS defeat system.

15. In addition to the ability impact the means of control of sUAS, the ability to destroy threats in flight is also necessary for a layered defense. While portable hand operated devices are available and can provide some degree of close protection, a fast-moving sUAS would be difficult to engage, particularly at night. As such, kinetic interdiction systems that are linked to the detection and tracking system are critical to ensure the defeat of sUAS. Currently, several options are available for this purpose including high-power microwave effectors, lasers, and the use of loitering interceptor sUAS. All of these systems have demonstrated merit but carry some risks if sensitive equipment is nearby. Of the options available, high-power microwave effectors have proven to be among the most reliable in defeating individual and swarms of sUAS but can have the largest negative impacts on nearby electronics.[25] The use of lasers, and interceptor sUAS have been extensively trialed, and leveraging the use of sUAS swarms to defeat a threat sUAS is also a possible future option.[26] While high-power microwave effectors may be one of the leading hard kill options at this time, a comprehensive sUAS defeat system must be able to incorporate new capabilities to keep pace with changing sUAS technology.

16. Like detection and tracking, it is important to leverage multiple defeat capabilities to eliminate threat sUAS. Failure to employ a layered system capable of employing multiple means to defeat sUAS could create a potentially exploitable weakness in the overall counter sUAS capability. It is also critical that automation can be achieved between the detection and defeat

[22] Georgia Lykou et al. "Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies." 14.

[23] Jie We, Jiaquan Ye, Jie Zou, Jing Gao, and Kaitao Cui. "Electromagnetic Interference Effect of the UAV Jamming Equipment on Instrument Landing System of Airport." In *2022 IEEE 5th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*. (2022). 958.

[24] Travis Cline and J. Dietz. "Agent Based Modeling for Low-Cost Counter UAS Protocol in Prisons." 5.

[25] Apartim Sharma "Counter-Unmanned Aircraft Systems (C-UAS): Future of Warfare." *Journal of Defence Studies.* Vol 16, Issue 4 (2022). 233.

[26] Martin Pozniak and Prakash Ranganathan. "Counter UAS Solutions Through UAV Swarm Environments." In *2019 IEEE International Conference on Electro Information Technology (EIT)*. (2019). 356.

systems to ensure that identified threats can be quickly defeated without the need for extensive and time-consuming human intervention in the process.

CONCLUSION

17. The threats posed by sUAS have rapidly increased as they have become more readily available and technologically complex. Based on global trends it must be assumed that the CAF will have to be prepared to respond to the sUAS threat on future operations and must therefore have capabilities to detect and defeat sUAS to protect soldiers, infrastructure, and equipment. As the CAF may encounter sUAS threats domestically as well, systems intended for use on deployed operations should also be capable of use within Canada as well.

18. While possessing a capability is a crucial step in employing it, the CAF has a great deal of work to do before using counter sUAS technologies in Canada and across the spectrum of conflict on deployed operations. Determining what needs to be protected, establishing where sUAS counter measures can be safely and legally employed, developing effective training for the use of the counter sUAS technologies selected, and integrating the CAF employed technologies and tactics with partner nations are some of the concurrent activities that must occur alongside the testing and procurement of effective counter sUAS technologies to ensure that the CAF is prepared to counter the growing sUAS threat.

RECOMMENDATION

19. To ensure the safety of CAF members, infrastructure, and equipment, it is essentially that counter sUAS technologies be procured. This technology must be capable of detecting and tracking threats through a scalable multi-sensor array and must be effective in defeating sUAS threats through a layered system of defense which employes multiple means of defeat to ensure the highest level of protection available.

BIBLIOGRAPHY

Besada, Juan A., Ivan Campaña, David Carramiñana, Luca Bergesio, and Gonzalo de Miguel. "Review and Simulation of Counter-UAS Sensors for Unmanned Traffic Management." *Sensors* (Basel, Switzerland) 22, no. 1 (2021). https://doi.org/10.3390/s22010189.

Brust, Matthias R., Grégoire Danoy, Daniel H. Stolfi, and Pascal Bouvry. "Swarm-Based Counter UAV Defense System." *Discover Internet of Things* 1, no. 1 (2021). https://doi.org/10.1007/s43926-021-00002-x.

Çetin, E., C. Barrado, and E. Pastor. "Improving Real-Time Drone Detection for Counter-Drone Systems." *Aeronautical Journal* 125, no. 1292 (2021). 1871–96. https://doi.org/10.1017/aer.2021.43.

Cline, Travis, and J. Dietz. "Agent Based Modeling for Low-Cost Counter UAS Protocol in Prisons." *International Journal of Aviation, Aeronautics, and Aerospace,* vol 7, issue 2, article 2, (2020). https://doi.org/10.15394/ijaaa.2020.1462.

Danczuk, Josef. "Bayraktars and Grenade-Dropping Quadcopters: How Ukraine and Nagorno-Karabakh Highlight Present Aid and Missile Defense Shortcomings and the Necessity of Unmanned Aircraft Systems." *The Military Review: The Professional Journal of the US Army*, (2023). 21-33. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/July-August-2023/Grenade-Dropping-Quadcopters/.

Lacher, Andrew, Jonathan Baron, Jonathan Rotner, and Michael Balazs. "Small Unmanned Aircraft: Characterizing the Threat." The MITRE Corporation, (2019). https://www.mitre.org/sites/default/files/2021-11/pr-18-3852-small-uas-characterizing-threat.pdf.

Lykou, Georgia, Dimitrios Moustakas, and Dimitris Gritzalis. "Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies." *Sensors (Basel, Switzerland)* 20, no. 12 (2020). https://doi.org/10.3390/s20123537.

Pozniak, Martin, and Prakash Ranganathan. "Counter UAS Solutions Through UAV Swarm Environments." *IEEE International Conference on Electro Information Technology (EIT)*, IEEE, (2019). 351-56. https://doi.org/10.1109/EIT.2019.8834140.

Samaras, Stamatios, Eleni Diamantidou, Dimitrios Ataloglou, Nikos Sakellariou, Anastasios Vafeiadis, Vasilis Magoulianitis, Antonios Lalas, et al. "Deep Learning on Multi Sensor Data for Counter UAV Applications-A Systematic Review." *Sensors (Basel, Switzerland)* 19, no. 22 (2019). https://doi.org/10.3390/s19224837.

Sharma, Apartim. "Counter-Unmanned Aircraft Systems (C-UAS): Future of Warfare." *Journal of Defence Studies.* Vol 16, Issue 4 (2022). 221-241. https://www.idsa.in/system/files/jds/jds-16-4_Apratim-Sharma_13.pdf.

Shoufan, Abdulhadi, and Ernesto Damiani. "Contingency Clarification Protocols for Reliable Counter-Drone Operation." *IEEE Transactions on Aerospace and Electronic Systems* 59, no. 6 (2023). 8944–55. https://doi.org/10.1109/TAES.2023.3313573.

US Department of Defence. "Army Techniques Publication No. 3-01.81: Counter-Unmanned Aircraft Systems (C-UAS)." Department of the Army, Washington DC. (2023). https://irp.fas.org/doddir/army/atp3-01-81.pdf.

Wallace, Ryan, Jon Loffi, Michael Quiroga, and Carlos Quiroga. "Exploring Commercial Counter-UAS Operations: A Case Study of the 2017 Dominican Republic Festival Presidente." *International Journal of Aviation, Aeronautics, and Aerospace* 5, no. 2 (2018): https://doi.org/10.15394/ijaaa.2018.1224.

We, Jie, Jiaquan Ye, Jie Zou, Jing Gao, and Kaitao Cui. "Electromagnetic Interference Effect of the UAV Jamming Equipment on Instrument Landing System of Airport." *IEEE 5th Advanced Information Management, Communicates, Electronic and Automation Control Conference*, IEEE, (2022). 955–59. https://doi.org/10.1109/IMCEC55388.2022.10020107.

Wilson, Bradley, Shane Tierney, Brendan Toland, Rachel M. Burns, Colby Peyton Steiner, Christopher Scott Adams, Michael Nixon, et al. "Small Unmanned Aerial System Adversary Capabilities." *Policy File*. RAND Corporation, 2020. https://www.rand.org/content/dam/rand/pubs/research_reports/RR3000/RR3023/RAND_RR3023.pdf.

Zakaria, Fareed. "Interview With President Volodymyr Zelenskyy and Mykhailo Fedorov About Ukraine's Army Of Drones and Ukraine's Children Of War." Fareed Zakaria Global Public Square, aired (2023). https://transcripts.cnn.com/show/fzgps/date/2023-09-10/segment/01.