Counter-measures against drone surveillance

S. Wong
R. Jassemi-Zargani
B. Kim
DRDC – Ottawa Research Centre

Defence Research and Development Canada

Reference Document
DRDC-RDDC-2016-D019
May 2016

IMPORTANT INFORMATIVE STATEMENTS

This publication has been published by the Editorial Office of Defence Research and Development Canada, an agency of the Department of National Defence of Canada. Inquiries can be sent to: Publications.DRDC-RDDC@drdc-rddc.gc.ca.

Abstract

Small drones are increasingly being used for spying/reconnaissance applications. They are small in size, making them hard to detect. They can be carried easily on a backpack, launched and recovered almost in any terrains. They are capable of providing real-time situational awareness information through live videos and high-definition pictures. Thus they can pose real and significant threats to military operations, such as those that are foreseen to be conducted by the CAF expeditionary force in the Arctic.

A survey is conducted on various methods for detecting the presence of small drones. A summary is given on the effectiveness of these methods. It is concluded that passive radar detection and radio-frequency detection hold good promise as useful techniques for countermeasures against drone surveillance.

Résumé

De plus en plus, on a recours à de petits véhicules aériens sans pilote (UAV) dans le cadre d'opérations d'espionnage et de reconnaissance. De taille réduite, ils sont difficiles à détecter et facilement transportables dans un sac à dos. Ils peuvent ainsi être lancés et récupérés sur quasiment tous les types de terrains. Les UAV permettent d'obtenir de l'information en temps réel sur la connaissance de la situation par l'entremise d'images vidéo en direct et en haute définition. Ils constituent donc une menace réelle et importante pour les opérations militaires, comme celles que devrait mener le corps expéditionnaire des FAC dans l'Arctique.

On procède à un sondage sur les diverses méthodes de détection des UAV de petite taille. Le résumé sur l'efficacité de ces méthodes révèle que les systèmes passifs de détection et les détecteurs de radiofréquences constituent des contremesures prometteuses relativement à la surveillance au moyen d'UAV.

Table of contents

List of figures

List of tables

This page intentionally left blank.

1 Introduction

Mini-UAVs and micro-UAVs are seen as a technology that is increasingly posing serious threats to military operations and public security. These unmanned flying systems are commonly referred to simply as drones. They are physically small in size, and light in weight. A typical drone such as the popular and ubiquitous quadcopter is less than 1 m in overall length or width, and weighs less than 15 kg in maximum take-off weight. Such drone system can be carried easily on the backpacks of ground troopers. The cost of a quadcopter system including sensors such as first-person-view video cameras (remote piloting) and HD cameras is relatively cheap, priced at less than $1000 per drone [1] and it is expected to fall as the market grows; thus it is an affordable and expendable item. This allows the users to push its operating envelop to the extreme limit, even to the point of sacrificing the drone when the acquisition of critical intelligence information is urgently sought.

Drones are expected to be used increasingly for scouting-spying and targeting purposes; they are useful for collecting and relaying real-time imagery on-the-fly, providing invaluable instantaneous tactical information in the battlespace. As a matter of fact, drones are reported being used by the Russians frequently in the Syrian conflict [2].

Battery-operated drones with range greater than 50 km are already available in the commercial hobby market [3]. The range performance is expected to improve as more efficient motors and higher capacity batteries are becoming available. It is also foreseen that SATCOM-capable drones will be available by 2020 as a technology trend [4]; this allows beyond line-of-sight communication between a low-flying drone and the ground controller stationed at a distance. For example, a drone flying at an altitude of 500 m (height of CN Tower) has a line-of-sight range of about 80 km; satellite data link allows a much greater stand-off distance for the controller.

Improvements in drone, sensor and data communication technologies will undoubtedly pose serious threats to the CAF's operations, especially those in the Arctic. It is foreseen that the CAF could deploy an expeditionary force patrolling the Arctic in the future to maintain sovereignty; this could potentially bring them in contact with foreign state-armed or privately-armed forces. Mobile forward operating bases for the CAF and sensitive operating areas will be vulnerable to foreign drone ISR activities. It is thus imperative for the CAF to be aware of any adversarial spying activities monitoring its operations [5]. Hence, a capability in countermeasures against drone surveillance will be necessary in order to provide security protection for the CAF to conduct their operations effectively in the Arctic.

2 Detection methods

There are a number of different approaches to drone detection. The following is a brief description of each of the methods summarizing the technology trends discussed on the internet. The focus is on the small drones that can provide real-time tactical information data. Also, they are very transportable, can be launched and recovered easily in any terrain, and are difficult to detect.

2.1 Audio detection

Noise from spinning propellers and electric motors can be detected by acoustic sensors such as microphones; but they have a limited range of about 100–150 m. A database of acoustic signatures from various drone models is compiled to discriminate ambient noises, preventing false alarm to set off. However, drone noise signature can be altered or muffled easily to defeat the database. Moreover, audio detection cannot be used to track target easily or accurately; it can only detect the presence of a drone in the vicinity and provides a warning. Nonetheless, audio sensors for detecting drones such as quadcopters are already commercially available for home privacy application [6] and commercial applications [7]. They are reported to have deployed around nuclear power plants and affluent neighbourhoods.

2.2 Video detection

Video cameras provide also a relatively short range detection, about 100 m [8]. It does not work well in misty, foggy conditions and at night. Because drones fly at low speed, around 16 m/s (58 km/hr), cameras may have difficulty distinguishing between drones and birds, especially when the birds are gliding. This may trigger an unacceptably high rate of false alarm. However, there may be AI (Artificial Intelligence) computer software available soon that may help to differentiate drones from birds on video/camera images through motion analysis.

2.3 Thermal detection

Thermal detection also has a range of about 100 meters and is subjected to weather conditions. Thermal shielding of the electric motors can further degrade the effectiveness of thermal detection. Most drones are built of plastic and carbon fibre materials. Thermal detection is found to be problematic in detecting these materials [8]. Infra-red cameras are more likely to pick up small birds due to their large thermal signatures, thus potentially causing a high rate of false alarm.

2.4 Radar detection

Conventional radar systems for drone detection are available. These systems can pick up drones which have radar cross-section (RCS) the size of small birds (0.01 m^2) at a range up to 2 km using very low transmitted power [9]. System that tracks small drones up to 20 km is claimed to exist [10].

However, there have been reports that radars have difficulties picking up small drone targets [8] [11] even though the drone RCS is within the detectable value. The problem is that subtle radar returns are hard to differentiate between those of a small drone and those from small birds and other sources of clutter. For drones that fly at low altitude and slow speed, unwanted clutters are problematic [12]. Furthermore, because birds have similar RCS as small drones, false alarm rate can be high. But with the advent of AI (artificial intelligence) technology, this problem may soon be solved in which an AI algorithm can differentiate a bird from a drone by analyzing the motion characteristic in the signals [12].

Another potential problem with radar detection is the requirement of continuous transmission of RF radiation. In an urban environment setting, placing a radar transmitter close to where people work and live may raise radiation health concerns. It may not be acceptable to the people living near the vicinity where a radar transmitter is emitting non-stop. Furthermore, the cost of operating a transmitter continuously 24/7 is another issue.

One potential use of radar detection in an urban setting is passive radar exploiting existing TV-signal towers as transmitters of opportunity. Firstly, TV-signals transmitted by major TV channels are powerful enough for detecting drones, even very small ones. Since TV transmission towers have been a fixture in the urban landscape for a long time, people are used to and accepting their presence. Secondly, TV-signal is free of charge; there is essentially no cost for tapping into the TV-signal transmission. Thirdly, TV-signals are transmitted continuously 24/7, making it an ideal source for radar surveillance application.

Using Ottawa as an example for passive radar detection of small drones in an urban setting, the TV-signal transmitter located at Camp Fortune can be exploited as a transmitter of opportunity to monitor critical high-value infrastructure assets against small drone spying activities. All of these target locations are within a 17 km radius from the TV transmission tower. For a small drone even the size of an insect (RCS = 0.001 m^2), passive radar using TV signal is capable of detecting such small targets. A sample calculation estimating the detection requirements is shown in Table 1. These requirements can be met readily using current COTS technologies.

Table 1: *Nano drone detection by passive radar over critical infrastructures using digital TV-signal transmission.*

Transmitter location	Camp Fortune, Quebec
TV transmission power, EIRP [19]	311 KW
Frequency (video carrier), f	537.25 MHz
Wavelength, c/f	0.558 m
Bandwidth, β	6 MHz
Distance from transmitter to target, R_1	17 km
Distance from target to receiver(s), R_2	1 km
Target Radar cross-Section, σ	0.001 m^2
Receiver antenna gain, G_R	100
Receiver antenna area, A	2.5 m^2
Received power	1.71×10^{-14} W
Noise power (receiver front end), η	2.85×10^{-14} W
SNR of received signal by receiver	0.6
Signal integration gain needed to achieve detection threshold $SNR_{DT} = 40$	67

Small drones operating near airports are raising safety concerns of planes flying in and out of the airports. Sightings of drones near the flight paths of jetliners are being reported more frequently and these drones are becoming a real hazard to air traffic. The TV tower at Camp Fortune has adequate power to detect insect-size drones in RCS (0.001 m^2) operating within a 5 km radius around the Ottawa International Airport. A sample calculation of the detection performance is shown in Table 2.

Table 2: *Nano drone detection by passive radar around the Ottawa International Airport using digital TV-signal transmission.*

Transmitter location	Camp Fortune, Quebec
TV transmission power, EIRP [19]	311 KW
Frequency (video carrier), f	537.25 MHz
Wavelength, c/f	0.558 m
Bandwidth, β	6 MHz
Distance from transmitter to target, R_1	30 km
Distance from target to receiver(s), R_2	5 km
Target Radar cross-Section, σ	0.001 m^2
Receiver antenna gain, G_R	100
Receiver antenna area, A	2.5 m^2
Received power	2.18×10^{-16} W
Noise power (receiver front end), η	2.85×10^{-14} W
SNR of received signal by receiver	7.64×10^{-3}
Signal integration gain needed to achieve detection threshold $SNR_{DT} = 40$	5236

2.5 Radio-Frequency (RF) detection

Using signals emitted by the drone is seen as another effective way to detect drones. There are already a number of companies marketing the idea and developing such systems [8] [13] [14] [15]. Detecting target RF emission signal is much easier because of the larger signal strength available to the sensors directly from the target. Some of the problems such as clutters and direct-path interference that are present in passive radar systems are also avoided.

A drawback of RF detection is that it must rely on the targets to transmit RF emissions. But this is not an overly detrimental factor that may render the method ineffective. Targets have to communicate with the ground controllers in navigation and in imagery collection. Even though drones can be pre-programmed to fly autonomously using GPS coordinates and pre-programmed to record video imagery and therefore emit no RF signals, the intelligence collected are likely to be regarded as sub-optimal and the information is considered as not as useful and desirable as real-time data. The main advantage of using small drone ISR systems is the ability to provide real-time situational awareness through real-time imagery. In modern battlespace, combatants rely on real-time information to understand the surrounding situations and react quickly to gain an advantage. Even in security monitoring applications, spying drones are mostly used to seek instantaneous situational awareness from the on-board camera imagery. The real-time demand means that most of the small drone missions would have to have constant communication link between the operators and the drones. Hence, RF detection is an effective way to detect the threats of drone surveillance by exploiting target RF emissions.

Because of the one-way RF propagation and RF emission is mostly omni-directional, RF emission can be detected using smaller equipment; these sensors are comparable to the portable automotive GPS receivers in size. Thus a RF detection system can be very mobile and transportable. This can be appealing to the CAF operating in the Arctic with an expeditionary force that is on the move frequently. RF detection can provide an effective counter-measures protection against drone reconnaissance by adversaries who must rely on real-time RF (communication) link, as pre-programmed GPS drones would neither be practical nor very effective in spying/scouting purposes against a mobile opponent.

In the case of applications for drone warning near airports, most of the threats will come from recreational activities of thrill-seeking amateur drone operators. The primary purpose in most of these cases is to use the on-board cameras to create first-person-view imagery in real-time by flying the drones close to in-flight aircraft for amusement. Thus, virtually all of these drones would be emitting RF signals. RF detection can provide accurate tracking of these drones and geo-locating the ground operators. Table 3 shows calculations for a typical commercial recreational drone transmitting video signal to communicate with the operator. It can be seen that it is quite feasible to pick up the emitted signal from a typical drone.

Table 3: *Detection of RF signal emitted by a typical drone target (commercial quadcopter).*

Drone transmitter power, EIRP [20]	0.1 W
Frequency (video carrier), f	5.8 GHz
Wavelength, c/f	0.055 m
Bandwidth, β	17.5 MHz
Distance from target to receiver(s), R	5 km
Receiver antenna gain, G_R	4
Received power	2.21×10^{-14} W
Noise power (receiver front end), η	8.5×10^{-14} W
SNR of received signal by receiver	0.26
Signal integration gain needed to achieve detection threshold $SNR_{DT} = 40$	154

Another potential application for RF detection is detecting and tracking nano-drones. Nano-drones are palm-size or smaller in physical dimensions (see Figures 1, 2). They can disguise their appearance as small birds, making them less conspicuous in hostile environments and harder to detect visually. These nano-drones can carry tiny cameras for surveillance and for remote piloting. Due to their small physical size, they are not able to carry adequate flight battery power to sustain flight longer than a few minutes; there may only be enough flight power capacity to get to and return from a designated target location. But these nano-drones can perch on tree branches and are capable of gripping onto a surface tightly to stay upright while watching a target area (see Figure 3). RF emissions will be transmitted to provide video image to the operator to find a suitable perching spot. Real time relay of imagery during surveillance will also produce RF emission. Thus, the presence and activities of nano-drones can still be detected even when they are not in flight. In addition, a perched drone cannot be detected by the radar detection method because a stationary drone would be buried among clutters of the surroundings.

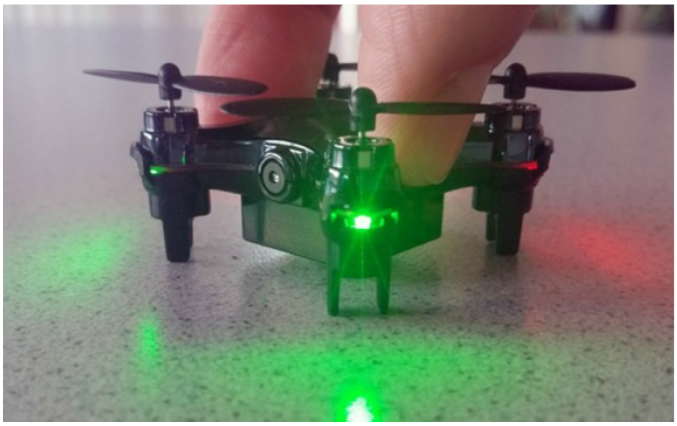

Figure 1: *A tiny eye in the sky [16].*

Figure 2: *Nano hummingbird; named one of the "50 best inventions of 2011" by TIME Magazine [17].*

Figure 3: *Drone with legs that can perch on a tree branch [18].*

For larger SATCOM capable drones, their RF emissions from datalink transmission of data to satellites can be detected and the drone's track can be monitored. Although their transmitting antennas will have greater directivity and will be pointing upward towards the satellites, their transmitting power is relatively high, around 7 W peak using the Iridium mobile phone handset as a reference. The sidelobe leakage power from the antenna will have sufficient power to be detected by ground sensors. Most sensors are very sensitive; as an example, as little as 10^{-16} W of the satellite signal can be detected by commercial GPS receivers that are used by automobiles on the roads. The current state-of-the-art detector sensitivity is 10^{-19} W. Moreover, the uplink signals from the drone to the satellites operate at a different frequency band than the downlink signals from the satellites; thus, the drone's transmitted signals are distinct to the RF detectors.

As commented in the Introduction, some drone ISR missions may push the operation envelop of the drones to the point of making the drones expendable in order to acquire the sought data. RF detection can provide an early detection of the drones, reducing the chance of success of such Kamikaze tactics. In brief, RF detection can offer a practical and effective tool for counter-measures against surveillance by drones of all types and sizes.

3 Summary

A survey is conducted on the trend of drone countermeasures methods. It appears that radar detection and RF detection are two effective approaches that hold promise for practical applications. In particular, passive radar exploiting TV-signal transmission looks especially viable for detecting threats posed by very small drones with RCS the size of an insect in urban settings. It is also possible to provide 24/7 monitoring with minimal operating cost since the radar illumination source (TV-signal) is already present in the ambient background and is essentially free.

Using the passive detection method already developed in the North Warning Systems study, target positions (i.e., GPS coordinates) can be determined and multiple targets can be tracked simultaneously in real-time [21]. This greatly facilitates the action of neutralizing the intruding drones by either hard-kill or soft-kill.

RF detection offers another reliable and effective means of detecting drones of all sizes, as long as the drones are emitting signals. Most of the anticipated scenarios will have the drones transmitting due to the nature of the drone's mission; for example, real-time spying/reconnaissance, operators deliberately flying their drones close to jetliners around airports. RF detection allows geolocation and tracking of multiple targets. In the case of drones flying near airports, drone operators on the ground can also be located by RF detection.

The advantage of RF detection is that no transmitter is required for target illumination. This means the detection system is much simpler, smaller and lighter, making it easier to be installed, un-installed, and moved around quickly. RF detection fits in the niche for a mobile drone countermeasures system that offers the CAF a capability to provide warning of spying activities on their operations.

The SIA/ICI-group has been conducting extensive modelling and simulation work on passive radar detection and RF detection concepts. The development is at a point where it is ready for experimental verification to assess and evaluate their practical potentials. An in-house project involving multi-sectional collaborative effort could be initiated to develop prototype systems as demonstrators. This would permit DRDC Ottawa to build up expertise and capability in the technology to support the CAF's future requirements.

This page intentionally left blank.

References

[1] DJI Phantom3 with 4K camera, http://store.dji.com/; accessed February 2016.

[2] "Russian defense minister: Syria operation shows drones are irreplaceable in modern warfare", TASS Russian News Agency, December 11, 2015, http://tass.ru/en/defense/843383; accessed January 2016.

[3] Microdrones model MD4-3000, https://www.microdrones.com/en/news/detail/microdrones-presents-the new-md4-3000/; accessed January 2016.

[4] "UAVs drive SATCOM modernization", October 26, 2010, http://www.defensemedianetwork.com/stories/uavs-drive-satcom-modernization/ accessed January 2016.

[5] "Arctic spy drones a defence concern as Russia expands reach", CBC News, February 11, 2015, http://www.cbc.ca/news/politics/acrtic-spy-drones-a-defence-concern-as-russia-expands-reach-1.2953027; accessed October 2015.

[6] "Drone Detection", https://gcn.com/articles/2015/06/03/drone-detection.aspx; accessed January 2016.

[7] "Japan's Alosk to launch warning system for unwelcoming drones", May 14, 2015; http://www.pcworld.com/article/2922552/japans-alsok-to-launch-warning-system-for-unwelcoming-drones.html; accessed February 2016.

[8] "Drone Detection: what works and what doesn't", May 28, 2015, www.net-security.org/article.php?id=2297&p=1; accessed January 2016.

[9] "ART Drone Sentinel", www.advancedradartechnologies.com/products-services/art-drone-sentinel; accessed January 2016.

[10] "Radars to prevent drone-aircraft collisions already in testing", December 8, 2014, www.eandt.theiet.org/news/2014/drone-aircraft-near-miss-radar.cfm; accessed November 2015.

[11] "Through the eyes of a radar: the visibility of UAVs to radar systems", 02.07.2015, Institute of High Frequency Technology, RWTHAachen University, https://www.microdrones.com/fileadmin/web/Images/Unternehmen/oeffentlichkeitsarbeit/UAVveek/presentation-documents/RCS_UAVveek.pdf; accessed January 2016.

[12] "Can we detect small drones like the one that crashed at White House?", February 3, 2015, http://spectrum.ieee.org/automation/robotics/arieal-robots/small-drone-detection-strategies; accessed November 2015.

[13] "Drone detection technology to watch over US airports", October 8, 2015, http://www.gizmag.com/us-faa-drone-detection-airport/39775/; accessed December 2015.

[14] Domestic Drone Countermeasures Inc., http://www.defenseone.com/technology/2014/11/military-wants-new-technologies-fight-drones/98387/; accessed January 2016.

[15] Drone Labs, http://www.dronedetector.com/compare-drone-detector/; accessed January 2016.

[16] Micro drone, http://www.gizmag.com/review-axis-drones-vidius/41605/; accessed January 2016.

[17] Nano hummingbird, http://www.avinc.com/nano; accessed January 2016.

[18] Perching drone, http://thefutureofthings.com/8574-bird-like-drone-actually-perches-spy/; accessed January 2016.

[19] http://tvfool.com/; accessed June 2015.

[20] https://www.firstpersonview.co.uk/transmitters/5.8ghz; accessed January 2016.

[21] R. Jassemi-Zargani et al., "ISR System-of-Systems concept evaluation of their effectiveness for NORAD Maritime Warning and the Replacement of the Aerospace Warning Systems", DRDC Scientific Report 2016, Publication is in progress.

DOCUMENT CONTROL DATA

(Security markings for the title, abstract and indexing annotation must be entered when the document is Classified or Designated)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g., Centre sponsoring a contractor's report, or tasking agency, are entered in Section 8.)

DRDC – Ottawa Research Centre
Defence Research and Development Canada
3701 Carling Avenue
Ottawa, Ontario K1A 0Z4
Canada

2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.)

UNCLASSIFIED

2b. CONTROLLED GOODS

(NON-CONTROLLED GOODS)
DMC A
REVIEW: GCEC DECEMBER 2013

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

Counter-measures against drone surveillance

4. AUTHORS (last name, followed by initials – ranks, titles, etc., not to be used)

Wong, S.; Jassemi-Zargani, R.; Kim, B.

5. DATE OF PUBLICATION (Month and year of publication of document.)

May 2016

6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)

22

6b. NO. OF REFS (Total cited in document.)

21

7. DESCRIPTIVE NOTES (The category of the document, e.g., technical report, technical note or memorandum. If appropriate, enter the type of report, e.g., interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Reference Document

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

DRDC – Ottawa Research Centre
Defence Research and Development Canada
3701 Carling Avenue
Ottawa, Ontario K1A 0Z4
Canada

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)

05EB

9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)

DRDC-RDDC-2016-D019

10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Unlimited

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

Small drones are increasingly being used for spying/reconnaissance applications. They are small in size, making them hard to detect. They can be carried easily on a backpack, launched and recovered almost in any terrains. They are capable of providing real-time situational awareness information through live videos and high-definition pictures. Thus they can pose real and significant threats to military operations, such as those that are foreseen to be conducted by the CAF expeditionary force in the Arctic.

A survey is conducted on various methods for detecting the presence of small drones. A summary is given on the effectiveness of these methods. It is concluded that passive radar detection and radio-frequency detection hold good promise as useful techniques for countermeasures against drone surveillance.

De plus en plus, on a recours à de petits véhicules aériens sans pilote (UAV) dans le cadre d'opérations d'espionnage et de reconnaissance. De taille réduite, ils sont difficiles à détecter et facilement transportables dans un sac à dos. Ils peuvent ainsi être lancés et récupérés sur quasiment tous les types de terrains. Les UAV permettent d'obtenir de l'information en temps réel sur la connaissance de la situation par l'entremise d'images vidéo en direct et en haute définition. Ils constituent donc une menace réelle et importante pour les opérations militaires, comme celles que devrait mener le corps expéditionnaire des FAC dans l'Arctique.

On procède à un sondage sur les diverses méthodes de détection des UAV de petite taille. Le résumé sur l'efficacité de ces méthodes révèle que les systèmes passifs de détection et les détecteurs de radiofréquences constituent des contremesures prometteuses relativement à la surveillance au moyen d'UAV.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g., Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

intelligence; Surveillance and Reconnaissance; Unmanned aerial vehicles; micro drones; nano drones; passive detection; countermeasures against surveillance