

Canadian
Forces
College

Collège
des
Forces
Canadiennes



COUNTER-UNMANNED AERIAL SYSTEMS : A CALL FOR ACTION TO PROTECT CANADIAN OPERATIONS ON DEPLOYED MISSIONS

Lieutenant-Colonel Jean-Marc Fugulin

JCSP 44

Exercice Solo Flight

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.

© Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence, 2019.

PCEMI 44

Exercice Solo Flight

Avertissement

Les opinions 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.

© Sa Majesté la Reine du Chef du Canada, représentée par le ministre de la Défense nationale, 2019.

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 44 – PCEMI 44

2017 – 2019

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

**COUNTER-UNMANNED AERIAL SYSTEMS: A CALL FOR ACTION TO
PROTECT CANADIAN OPERATIONS ON DEPLOYED MISSIONS**

By Lieutenant-Colonel Jean-Marc Fugulin

“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 diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale. »

\

INTRODUCTION

Unmanned Aerial Systems (UAS) represent a real and growing threat to Canadians when deployed on overseas operations as presented to the Canadian Joint Operations Command staff by Colonel Chris McKenna, commander Task Force Mali, Roto 0:

A new trend observed is the use of Unmanned Aerial System (UAS) to conduct observation of Camp Castor¹ and other MINUSMA² and military installations in Mali. The quality of quantitative data is at this time very low within MINUSMA due to a lack of proper UAS awareness, identification and reporting but all agree that terrorists have recently procured and developed techniques to conduct reconnaissance of bases. While no armed drones have been found to date, it is likely that Terrorist Armed Groups (TAGs) are currently working at weaponizing UAS as it is done in the Middle East.³

Unmanned Aerial System (UAS) flying over Mali's Operation *Presence* military camp is a worrying threat for which the Canadian Task Force is ill-equipped to address. In effect, the Canadian Armed Forces lack counter-UAS doctrine, training, detection system, equipment, ROEs, and tactics, technics and procedures (TTPs) to protect its personnel, equipment and facilities.

This paper argues that the CAF should speedily develop an initial counter-UAS capability for use in their deployed camps. The paper begins with an overview to situate and understand the threat, the environment and the need for counter-UAS in a deployed

¹ Camp Castor is the camp occupied by the Task Force Mali is Gao.

² *Mission multidimensionnelle intégrée des Nations Unies pour la stabilisation au Mali*. Details on this mission can be found at <https://peacekeeping.un.org/en/mission/minusma>.

³ Col. Chris McKenna, "Mission Backbrief to CJOC Staff", Op PRESENCE TF Mali, 4 Feb 19.

setting. In particular, it will leverage the experience from the Operation *Presence* - Mali Roto 0 at camp Castor to illustrate challenges, risks and threats facing a current Canadian mission. The Mali case of UAS will then be analysed through a force protection vulnerability assessment. Factors and deductions extracted from the analysis will then be discussed and presented using the DOTMLPF⁴ framework. Such an examination will illustrate a capability gap for which there is a pressing need for the CAF to adopt a counter-UAS strategy for their deployed camps.

The intent of this paper is to focus on one particular aspect of counter-UAS, the threat to Canadian military housed in camp installations when deployed overseas. When at home, the responsibility for counter-UAS is deferred to the RCMP as in the case during Operation *Cadence* during the G7 summit in 2018 in Charlevoix, Quebec.⁵ The same strategy cannot be adopted when abroad since the RCMP does not have jurisdiction, hence the need for the CAF to obtain a counter-UAS capability.

THE SITUATION

Small unmanned aerial systems, also referred to as drones, have been proliferated around the world and are now used in illicit activities. Examples include usage in proximity of airports, critical infrastructures, security-controlled zones, and high-profile events, sparking safety concerns. More particularly, the usage of drones in a combat

⁴ As per the NATO definition of Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities. <https://www.act.nato.int/acronyms>

⁵ Government of Canada, *Operation Cadence*. Last accessed 17 May 2019. <https://www.canada.ca/en/department-national-defence/services/operations/military-operations/recently-completed/operation-cadence.html>

function is not the sole prerogative of technologically advanced states since commercially and readily available drones have opened the possibility for extremist groups to access air power. These hostile *pseudo-Air Forces* are posing a security threat to the deployed personnel, equipment and infrastructure. In effect:

With the development of UAVs (...) insurgent may now have a near-equal knowledge of the enemy's deployment on the battlefield or the defensive measures being deployed against them at a targeted military base.⁶

UAS comes in a wide variety of sizes and types, offering an array of air power effects. This paper will focus on the Class I (weight less 150kg), which include small, mini and micro UAS.⁷

TYPES OF UAS THREATS

Small drones are used by insurgents and terrorists to “allow asymmetrical approaches to conduct attacks, collect information, or trigger other threatening events.”⁸ Many articles and papers have covered the development of UAS usage in conflicts over the last fifteen years in areas such as Israel, Middle-East, Ukraine, Syria, Iraq and now Africa. The intent of this paper is not to review the historical development of the UAS usage in conflict, but rather to provide an overview of some of the key developmental stages in order to frame the UAS threat challenges currently facing the CAF.

⁶ Abbott et al, *Hostile Drones: Supplementary Risk Assessment* (London, Oxford Research Group, 2016), 4.

⁷ As defined by the NATO Classification system, which is the system adopted by the CAF.

⁸ United States. Department of the Army. ATP 3-01.81, *Counter-Unmanned Aircraft Systems Techniques*. Washington, DC: Department of the Army, April 2017, 1-1.

Insurgents and terrorists have developed and perfected their tactics and are using UAS for two primary purposes: intelligence, surveillance and reconnaissance (ISR) and attack.⁹

Threats will be grouped into five categories that will be used later in the analysis, and are described as follows:

Type I Threat – As an ISR Platform

From an ISR perspective, almost all low cost drones are equipped with camera that can “easily gather critical information about unit composition, pattern of life and troop movement.”¹⁰ First-person view flying has grown in capability and flight control over line of sight is accomplished by means of a live video down link displayed on smart phones.¹¹

Type II Threat – As a Weapon Delivery Platform

With increasing payload capability, weaponized drones have started to be used by belligerents in the battlefield with success. Drones are used as a delivery mechanism for improvised explosive devices (IED) such as demonstrated by ISIS dropping grenades over a Syrian Army ammunition storage in October 2017.¹² Other instances include the bombing of Kurdish and French positions successfully injuring soldiers in 2016¹³ and during the clearing of Mosul.¹⁴ As insurgents develop their air capabilities, the UAS

⁹ Major Dan Walters, “Countering the Small-Unmanned-Aircraft-System Threat to the Canadian Armed Forces,” *Royal Canadian Air Force Journal* 5, no. 4 (Fall 2016): 6.

¹⁰ David J. Praisler, “Counter-UAV Solutions for the Joint Force” (research paper, Air War College, April 6, 2017), 9, accessed January 7, 2019, 6.

¹¹ *Ibid.*, 8.

¹² Master Corporal Alexandre Pelletier, “Counter-Unmanned Aircraft Systems for the Royal Canadian Air Force,” *Canadian Forces School of Aerospace Studies*, 2018 Manson Award, 1.

¹³ Kelsey D. Atherton, “IED Drone Kills Kurdish Soldiers, French Commandos,” *Popular Science*, 11 October, 2016. Last accessed 16 May 2019 <https://www.popsci.com/booby-trapped-isis-drone-kills-kurdish-soldiers-french-commandos>

¹⁴ Joby Warrick, “Use of weaponized drones by ISIS spurs terrorism fears,” *The Washington Post*, 21 February 2017. The article also shows evidence found in propaganda video footage. <https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs->

threat continues to “evolve in application, scope and complexity”¹⁵. Open source reported that rebels in Syria targeted Russian installations with dozens of weaponized drones and that “swarm-like attacks using weaponized drones is a growing threat and likely to only get worse.”¹⁶

Type III Threat – As Targeting Tool

It was reported that Ukrainians and pro-Russian forces used UAS in relatively large numbers “each functioning at different altitudes with various sensor packages designed to complement each other’s capabilities.”¹⁷ Drone information was used to correct artillery fire to improve targeting accuracy.¹⁸ Further, modern models incorporate onboard GPS receivers enabling not only autonomous navigation, but when combined with video capability, provide a powerful targeting tool:

The adversary will now have near real time geo-referenced video available which can be combined with GPS guided rockets, artillery, mortars and missiles to conduct rapid and accurate attacks.¹⁹

terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html?noredirect=on&utm_term=.9442d1fa08de

¹⁵ Ryan Wallace et al., “Exploring Commercial Counter-UAS Operations: A Case Study of the 2017 Dominican Republic Festival Presidente” *International Journal of Aviation, Aeronautics, and Aerospace*, Vol 5 Issue 2 (2018), 19.

¹⁶ Jeff Daniels, “Russia says it killed rebels behind swarm drone attack in Syria, but experts see more such strikes ahead,” (Jan 2018) *CNBC News*. <https://www.cnbc.com/2018/01/12/russia-says-it-eliminated-rebels-behind-swarm-drone-attack-in-syria.html>

¹⁷ Lamport, Jeffery; Scotto, Anthony, “Countering the UAS Threat: A Joint Perspective,” *Defense Systems Information Analysis Center*, 3. Last accessed 20 May 2019. <https://www.dsiac.org/resources/journals/dsiac/fall-2016-volume-3-number-4/countering-uas-threat-joint-perspective>

¹⁸ John Wendle, “The Fighting Drones of Ukraine,” *Air & Space Magazine Smithsonian*, February 2018, last accessed 18 May 2019 <https://www.airspacemag.com/flight-today/ukraines-drones-180967708/>

¹⁹ William Selby, “Operating in an Era of Persistent Unmanned Aerial Surveillance,” *Small Wars Journal*, 2. Last accessed 17 May 2019. <https://smallwarsjournal.com/jrnl/art/operating-in-an-era-of-persistent-unmanned-aerial-surveillance>

Type IV Threat – As Command and Control Tool

Open source reports that ISIS used drones to aid local leaders in making real-time tactical-level decisions, to “help guide vehicle-borne IEDs more accurately toward their targets,”²⁰ effectively influencing in real time the location and time of the explosion to maximize destruction. Drones used in a command and control role are especially effective in an urban area where a suicide bomber has difficulty navigating, but “with the help of a drone a path for directly reaching the target can be easily determined.”²¹ The efficiency of the attack is also increase when it is the drone operator who “decides the timing of an attack rather than a suicide bomber who has limited view and is nervous.”²² A similar tactic was used whilst coordinating a breach attack on coalition camps, maximizing the breach and capitalizing the shock and chaos situation.

Type V – As Propaganda Tool

Drone videos offer a privileged platform that can be broadcasted for media propaganda over the internet. Aerial footages of successful attacks are channeled to media and social media to show casualties and resulting chaos.²³ They easily enhanced the insurgent’s strategic communications strategy.²⁴

²⁰ Arthur Holland Michel, “Counter-Drone Systems.” Center for the Study of the Drone at Bard College, February 20, 2018, 1.

²¹ Serkan Balkan, “Daesh’s Drone Strategy Technology and the Rise of Innovative Terrorism,” SETA Publications, Istanbul, Turkey, 2017, 24.

²² Ibid., 33.

²³ Ibid., 38.

²⁴ Dan Rassler, “Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology,” United States Military Academy, West Point, NY, October 2016, 12.

THREAT LEVELS

According to the world's first civil society intelligence agency, Open Briefing, the overall hostile drone usage risk is rated as "High" from insurgents and "Medium High" from terrorists, both ratings are in the *red category*, meaning representing an unacceptable level of risk requiring a response strategy.²⁵

OPERATION PRESENCE

The Operating Environment

Operation *Presence* – Mali is the Canadian Armed Forces (CAF) participation to the United Nations Multidimensional Integrated Stabilization Mission in Mali (MINUSMA), and is part of the Government of Canada's overall efforts to help set conditions for durable peace, development, and prosperity in Mali.²⁶ Located directly adjacent to the Gao airport, Camp Castor houses the Canadian contingent and is approximately 800,000 square meter area in size. It is neighbour to a *Super Camp*, housing various United Nations (UN) contingents, and in the vicinity of a Malian Air Force Base, a Chinese Camp and a French Camp under *Opération Barkhane*. In particular, the Canadian helicopter detachments working areas are concentrated near the apron and flight line. The contingent shares general living areas with personnel from other nations, such as Germany, Belgium, Netherlands and France. Further, there are 31

²⁵ OpenBriefing, "Hostile Drones," Last accessed 25 May 2019.
<https://www.openbriefing.org/publications/report-and-articles/hostile-drones-supplementary-risk-assessment/>

²⁶ Government of Canada, *Operation PRESENCE – Mali*. Last accessed 17 May 2019.
<https://www.canada.ca/en/department-national-defence/services/operations/military-operations/current-operations/op-presence.html>

UN agencies and international Non-Governmental Organizations (NGOs) operating in GAO.²⁷

The UAS Threats in Mali

As discussed previously, current technological and manufacturing advancements are creating a situation where terrorists and insurgents have access to reliable and cheap drone technology.²⁸ Evidence shows that rebel groups in Mali are using drones for collecting information on the United Nations, Camp Castor and the Canadian installation. They have not yet weaponized the use of UAS, but it is only a matter of time for that level of threat to migrate to Africa.²⁹ As a side note about Syria and Iraq, open source reported that that technological advancement from ISIS with UAS use were extensive and fast; a mere two years after introducing them for surveillance purposes, they used UAS to drop bombs onto Iraqi troops in Mosul. Using this observation as a guiding trend, one can forecast that weaponized drones could start appearing into the Sahel region within the next two to three years. Finally, rebel groups in Mali have released video footage from drone operations on the internet as part of their propaganda.³⁰

Not All UAS are Hostile

In Gao, drones are being used on an almost daily basis by the UN, other nations and NGOs as part of their operations. As both hostile and friendly UAS are using

²⁷ United Nations, Mali : Presence of UN Agencies and International NGO, Nations Unies, Bureau pour la coordination des affaires humanitaires (UNCHA) report. https://reliefweb.int/sites/reliefweb.int/files/resources/ocha_nord_presence_cercle_20160310_en_0.pdf

²⁸ Mike Armstrong, "Drone Wars: Is Canada's Military Prepared for Weaponized Drones?" Global News, May 29, 2018, 1. <https://globalnews.ca/news/4240532/drone-wars-is-canadas-military-prepared-for-weaponized-drones/>

²⁹ "The parties that are hostile to the UN have used drones over UN camps," said Walter Dorn. "But so far, not for using explosives." Ibid., 2.

³⁰ Ibid.

commercially available models, all drones appear alike from an outlooker. This situation increases dramatically the task of detecting hostile drones, which is a recurring problem at Camp Castor. Because of all the different agencies with own mandates working alongside each other, sightings by personnel working in different organizations are most of the time not reported. MINUSMA does not currently have a defence system able to combat the UAS threat. The usage of friendly and neutral UAS in Mali are not registered and uncoordinated. The UN started issuing directives to guide initial reactions to drone sightings, but much work is required before an accurate portrait on the extent of the situation can be made. Official reporting of suspected UAS flights report sighting on a monthly basis, but it is believed that the real number is far more than that. UAS flight path procedures are in the process of being implemented to help in managing friendly UAS and in detecting hostile ones. No result from that initiative is known at this time.

RISK ANALYSIS

Researchers on terrorism risk, such as Willis, depicts risk as the product of threat, vulnerability, and consequences as reproduced at Figure 1, in which threat is defined as the “probability that a specific target is attacked,” vulnerability as “the probability that damages occur under an attack,” and consequences as “the expected magnitude of damage (e.g., deaths, injuries, or property damage)”³¹

³¹ Henry H. Willis, “Guiding Resource Allocations Based on Terrorism Risk,” *Risk Analysis*, Vol. 27, No. 3, 2007, 598-599.

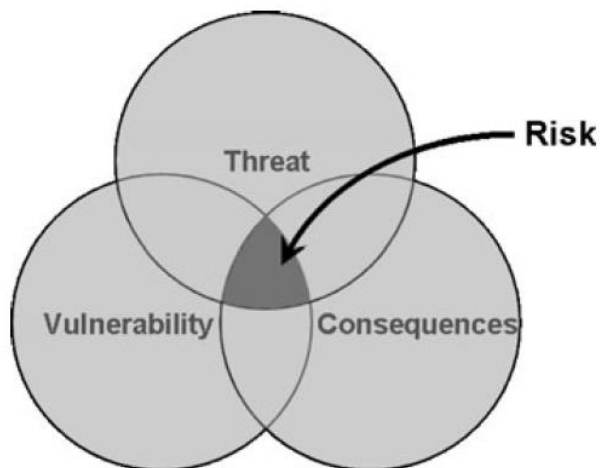


Figure 1 – Risk is the Intersection of Threat, Vulnerability and Consequence
 Source: Willis, Guiding Resource Allocations Based on Terrorism Risk, 598

The Canadian Joint Force Protection doctrine utilizes the Threat-Vulnerability-Risk Assessment (TVRA) process to enable commanders and staffs to safeguard assets and respond to attacks.³² The evaluation of risk includes a criticality assessment which “permit risk analysis to be conducted by considering the likelihood and impact of a threat exploiting a vulnerability to an asset that is critical to mission success.”³³

Methodology Used

The CARVER (criticality, accessibility, recovery, vulnerability, effect, and recognition) matrix will be used as a support tool to perform the TVRA.³⁴ The CARVER

³² Department of National Defence, B-GJ-005-314/FP-000, CF Joint Force Protection Doctrine (Ottawa: DND Canada, 2006), 7-1.

³³ Ibid. 7-2

³⁴ Christopher M. Schnaubelt, Eric V. Larson, and Matthew E. Boyer, “Vulnerability Assessment Method Pocket Guide” RAND Corp (2014), 107. Another available tool is the MSHARPP (mission, symbolism, history, accessibility, recognizability, population, and proximity).

analysis ranks vital assets along the six mentioned force protection criteria and is reproduced at Annex A.

Countering the Threat

Numerous works has been published on counter-UAS technology alongside an emerging array of commercial solutions poised to mitigate the growing threat of hostile drone usage. The technology faces the problem with two methods, detection and engagement. Detection encompasses the means to “detect, locate, track, and identify an unmanned aircraft” as engagement involves technology and actions to “prevent, disrupt, disable, override, spoof [mislead], or otherwise interfere with UAS operations.”³⁵ Engagement can also incorporate active measures to “capture, inflict damage, or destroy the aerial vehicle”. It is important to note that the latter actions are not clearly legislated, with hurdles over a complex set of overlapping jurisdictions and legislation topics.³⁶ For example, signal jamming devices are either illegal or restricted in most developed countries.³⁷ In parallel to the legal framework, countering UAS also present challenges in other diverse subjects as “the massive development of UAS technology is outgrowing user, legal, moral, and military-political frameworks.”³⁸ Counter-UAS systems should be

³⁵ Ryan Wallace et al., “Exploring Commercial ...,” 3.

³⁶ Jonathan Rupprecht, “7 Big Problems with Counter Drone Technology (Drone Jammers, Anti Drone Guns, etc.),” Rupprecht Law, P.A. Last accessed on 18 May 2017 <https://jrupprechtlaw.com/drone-jammer-gun-defender-legal-problems#legal>

³⁷ Holland Michel, Arthur. “Counter-Drone Systems...,” 8.

³⁸ Kratky, Miroslav and Jan Farlik. "Countering UAVs - the Mover of Research in Military Technology." *Defence Science Journal* 68, no. 5 (Sep, 2018): 461. <https://search.proquest.com/docview/2131597131?accountid=10524>

employed force wide as a new means for security forces to maintain control and safety over critical assets.³⁹

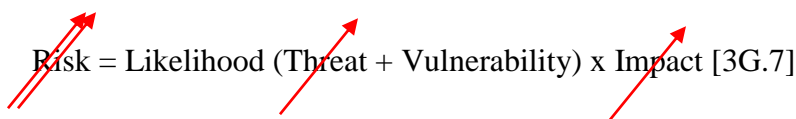
DISCUSSION

High Risk Assets

The CARVER matrix lists in order of criticality the vital assets found in a deployed setting that is typical of a current operational Theatre in which the CAF are involved. The threat-vulnerability-risk assessment aligns the criticality of assets against the likelihood of attack under a threat scenario, in this case typical of a UN African mission, and sees four assets as being identified at high risk from hostile UAS operations: personnel, aircrafts, camp access control points, and mess/accommodations. Medium risk assets include landing area/taxiway, fuel storage, hangars and ammo depot.

The Need to Decrease Our Vulnerability

Risk is generally described as likelihood times impact, and particular to the security domain, likelihood is a combination of threat and vulnerability. With this in mind, the increasing risk posed by the development of hostile UAS in a deployed setting can be viewed as having the following effect:

$$\text{Risk} = \text{Likelihood} (\text{Threat} + \text{Vulnerability}) \times \text{Impact} \text{ [3G.7]}$$


Red arrows: The growing trend of UAS usage by insurgents and rebels against deployed operations increases both *threat* and *impact* as described previously. When no counter-

³⁹ David J. Praisler, "Counter-UAV Solutions..." 17.

UAS capability is available, as the case currently with the CAF, vulnerability stays the same, hence risk elevates (depicted as the double red arrows).

$$\text{Risk} = \text{Likelihood (Threat + Vulnerability)} \times \text{Impact [3G.7]}$$

Blue arrows: Vulnerability is the component of risk over which “the commander has the most control and greatest influence.”⁴⁰ Therefore, to keep the level of risk low, vulnerability of critical assets must be protected against UAS to compensate for the combined effect of a higher threat and a higher impact (depicted as the double blue arrows).

When deployed within a US-led coalition, Canada can operate safely under a well-established counter-UAS umbrella, which is not the case when deploying on a peacekeeping mission in Africa. In Gao for example, the Germans are trying to enhance their air defence system to cope with the UAS threat on behalf of the UN.⁴¹ Anecdotal evidence hints that the system is not yielding the expected counter-UAS result.⁴² If Canada wish pursuing a greater peacekeeping role in Africa as a main player or as a lead contributing nation, the responsibility for an efficient counter-UAS will fall on us.

⁴⁰ Christopher M. Schnaubelt, “Vulnerability Assessment Method...,” 106.

⁴¹ Written by DefenceWeb - 21st Jan 2019 UN deploys RADA radars in Mali
<https://www.defenceweb.co.za/featured/un-deploys-rada-radars-in-mali/>

⁴² Emails Cyr-Fugulin and Stewart-Fugulin dated May 2019.

Government of Canada Counter-UAS Efforts

Several Government of Canada Departments are poised with the issue of counter-UAS but none has yet institutionalized it; the Government has not decided which organization will champion this task as the issues for protecting against malicious drone activities are very complex, and the UAS technology is evolving faster than our ability to understand the threat and implement counter measures. The RCMP uses different systems trialed on a case-by-case basis and tailored to the task at hand, such as providing security during high profile events. Correctional Services Canada (CSC) is currently searching for “an innovative and cost-effective technology solution to detect, track and prevent contraband items from entering the perimeter via Unmanned Aerial Vehicle (UAV).”⁴³ Mandated by CSC, the Defence Research and Development Canada (DRDC) completed a study on commercially available solutions for counter-UAS, but even though solutions are available, they “don't include legal and safe counter measures and are too expensive for CSC to deploy to all its institutions.”⁴⁴ At the moment, CSC is focusing on the detection of illicit drone activity, with radar systems being the most promising mean of detection.

As with the CAF, expertise is being developed and initiatives are being trialed, but only at localized levels. The Department of National Defence has organized a DND Unmanned Aircraft Systems Working Group to look at both the drone and anti-drone issue. NORAD is currently looking at synchronizing efforts being confronted with North-American air space control and airworthiness issues related to illicit use of drones.

⁴³ Government of Canada, Preventing Contraband Delivery via Air and Ground request for proposal, last accessed 20 May 2019. <https://www.ic.gc.ca/eic/site/101.nsf/eng/00042.html>

⁴⁴ Ibid.

Bottom line being that the force protection issue of counter-UAS in deployed operations is not addressed at the moment by the CAF, leaving our personnel, assets and facilities at risk.

ROAD AHEAD

Since an overall DND counter-UAS strategy will not be available soon, the CAF should prioritize the implementation of solutions for protecting deployed camps, personnel and assets as they face current, real and increasing threats posed by UAS. Since the current trend is towards peacekeeping missions in Africa, it situates us in locations where we cannot rely on a coalition framework to counter the UAS threat for us. CAF force protection specialists and Engineers should lead in finding adapted solutions to this problem as highlighted during Operation *Presence* – Mali. To do so, some of the proposed areas of development are as follows:

Doctrine and TTPs

Doctrine is necessary to guide action and to provide a common framework spanning all levels of conflict so that planners, decision-makers and operators can deliver effects. Rather than developing an all-encompassing one, counter-UAS for deployed camps should build upon current force protection guidelines by introducing an annex describing over-guiding principles in counter-drone activities applied to overseas situations. From there, theatre specific TTPs could be developed in a view to implement mitigations measures on time for the next theatre of operations.

Organization

As experienced in Mali, the first step in addressing threats from drones is to develop a strong discipline towards friendly UAS flight management discipline. Although flight

clearances for UAS can be perceived as restrictive, “they are critical to ensuring other friendly forces in the area do not engage those UASs.” The CAF should ensure to deploy expertise to contribute in the management of the Area Air Defense Plan (AADP) with local airspace coordinating measures incorporating actions for UAS control.⁴⁵

Training

The first step in an effective defence against hostile drone is to ensure adequate and early detection. To do so, personnel should be trained to “understand [terrorists UAS] capabilities and employment doctrine, predict where and how they will be employed, and identify their most likely targets.”⁴⁶

Material

Counter-UAS technology is extremely varied – there are currently 115 different systems commercially available listed within the counter-UAS online directory.⁴⁷ Looking at a counter-UAS solution is outside the scope of the present essay, but leveraging current local initiatives within the Special Forces, RCMP or CSV and/or duplicating systems already in operations within a coalition environment where the CAF participates, are hints for capabilities to trial in a realist timeframe.

Leadership & Education

The CAF should change its reactive posture into a proactive attitude towards hostile counter-UAS, especially since “an active role in AADP development to ensure it adequately mitigates threats to the maneuver force.”⁴⁸

⁴⁵ Lamport, Jeffery, “Countering the UAS...,” 5.

⁴⁶ Ibid.

⁴⁷ UnmannedAirspace.info, “Counter UAS Directory, version 1” March 2018. Last accessed 19 May 2019. <https://www.unmannedairspace.info/counter-uas-industry-directory/>

⁴⁸ Lamport, Jeffery, “Countering the UAS...,” 5.

In addition, legal parameters should be framed, such as basic UAS-specific rules of engagement, such that “identification and engagement authority for low, slow, small UASs should rest at the lowest possible tactical level.”⁴⁹ The legal framework should also ensure that criteria for “hostile act” and “hostile intent” addressing UAS threat are written in simple terms language addressing troop protection.

Personnel

The deploying task force should include personnel qualified in counter-UAS. In addition, all task force personnel should receive pre-deployment training on UAS threat, protection and sighting reporting procedures.

Facilities

Camp force protection should be designed for and incorporate counter-UAS measures adapted to the threat with a focus on protecting vital assets as per a priority list proposed by specialists alongside a risk assessment analysis to be vetted by the Task Force Commander.⁵⁰ Risk mitigation solutions can then be put in place ranging from concealment⁵¹, hardening, passive and active defence systems.

⁴⁹ Ibid.

⁵⁰ As mentioned in US doctrine ATP 3-01.81, counter-UAS is a Commander’s responsibility.

⁵¹ Kelsey D. Atherton, “IED Drone Kills Kurdish Soldiers, French Commandos,” *Popular Science*, Oct 2016, 2. Last accessed 20 May 2019. <https://www.popsci.com/booby-trapped-isis-drone-kills-kurdish-soldiers-french-commandos>

CONCLUSION

“The time for admiring the problem must reach an end.... The threat is here and cannot be allowed to put our assets and personnel at risk; the capabilities are available; the methodology is sound; it is time to act.”⁵²

The threat is current, real, present and growing as insurgents are targeting UN and Canadians in Mali. It is only a matter of time for weaponized UAS to migrate from the Middle-East to Africa. The CAF should adopt a more pro-active posture in managing unwanted drone activity on deployed operations with a counter-UAS capability. Short term objectives should include UAS recognition, pre-deployment training, and development of Canadian TTPs for deployed operations focusing on the Sense function (i.e. detect). Leveraging expertise from other governmental departments should be examined as a mean to attain an initial operational capability delivering some protection for peacekeeping missions in Africa. Establishing common guidelines, criteria and follow-on actions with the deployed stakeholders; in the case of Mali, this includes the UN, the OGDs, as well as the German, French, Dutch and Japanese contributing nations. In conclusion, the CAF should develop swiftly a counter-UAS capability to protect its deployed vital assets' vulnerability against an increasing threat and impact from hostile drones' usage, typical of a peacekeeping employment scheme in Africa.

⁵² David J. Praisler, “Counter-UAV Solutions...,” 22.

ACKNOWLEDGMENTS

I would like to thank Major Jean-David Cyr, Captain Dave Beatty and Mr. Tom Stewart for providing valuable information on particulars for Task Force Mali – Roto 0 and a wealth of information on the current CAF situation vis-à-vis UAS.

BIBLIOGRAPHY

Primary

Abbott et al. "Hostile Drones: Supplementary Risk Assessment." London, Oxford Research Group, 2016.

Armstrong, Mike, *Global News*, "Drone Wars: Is Canada's Military Prepared for Weaponized Drones?" Last modified 29 May 2018.
<https://globalnews.ca/news/4240532/drone-wars-is-canadas-military-prepared-for-weaponized-drones/>

Atherton, Kelsey D., *Popular Science*, "IED Drone Kills Kurdish Soldiers, French Commandos." Last modified Oct 2016. <https://www.popsci.com/booby-trapped-isis-drone-kills-kurdish-soldiers-french-commandos>

Balkan, Serkan. "Daesh's Drone Strategy Technology and the Rise of Innovative Terrorism." SETA Publications, Istanbul, Turkey, 2017.

Canada. Department of National Defence. B-GJ-005-314/FP-000, *CF Joint Force Protection Doctrine* Ottawa: DND Canada, 2006.

Canada. Government of Canada. *Operation CADENCE*. Last accessed 17 May 2019.
<https://www.canada.ca/en/department-national-defence/services/operations/military-operations/recently-completed/operation-cadence.html>

Canada. Government of Canada. *Operation PRESENCE – Mali*. Last accessed 17 May 2019. <https://www.canada.ca/en/department-national-defence/services/operations/military-operations/current-operations/op-presence.html>

Canada. Government of Canada. *Preventing Contraband Delivery via Air and Ground request for proposal*. Last accessed 20 May 2019.
<https://www.ic.gc.ca/eic/site/101.nsf/eng/00042.html>

Cowan, Gerrard. "The Twists and Turns of Countering UAVs." *Armada International* 42, no. 6 (Dec, 2018): 24-26.

Cyr, Jean-David, Collection of Information on Camp Castor (2019).

Daniels, Jeff, *CNBC News*, "Russia says it killed rebels behind swarm drone attack in Syria, but experts see more such strikes ahead." Last modified Jan 2018.
<https://www.cbc.com/2018/01/12/russia-says-it-eliminated-rebels-behind-swarm-drone-attack-in-syria.html>

- Holland Michel, Arthur. "Counter-Drone Systems." Center for the Study of the Drone at Bard College, February 20, 2018.
- Kratky, Miroslav and Jan Farlik. "Countering UAVs - the Mover of Research in Military Technology." *Defence Science Journal* 68, no. 5 (Sep. 2018): 460-466.
- Lamport, Jeffery, and Anthony Scotto, *Defense Systems Information Analysis Center*, "Countering the UAS Threat: A Joint Perspective" Last accessed 20 May 2019. <https://www.dsiac.org/resources/journals/dsiac/fall-2016-volume-3-number-4/countering-uas-threat-joint-perspective>
- McKenna, Chris. "Mission Backbrief to CJOC Staff", *Op PRESENCE TF Mali*, 4 Feb 19.
- OpenBriefing*, "Hostile Drones." Last accessed 25 May 2019. <https://www.openbriefing.org/publications/report-and-articles/hostile-drones-supplementary-risk-assessment/>
- Pelletier, Alexandre. "Counter-Unmanned Aircraft Systems for the Royal Canadian Air Force." Canadian Forces School of Aerospace Studies, 2018 Manson Award.
- Praisler, David J. "Counter-UAV Solutions for the Joint Force" Air War College, Research Paper, April 2017.
- Rassler, Dan. "Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology." United States Military Academy, West Point, NY, October 2016.
- Rupprecht, Jonathan. "7 Big Problems with Counter Drone Technology, Drone Jammers, Anti Drone Guns, etc." Rupprecht Law, P.A. Last accessed on 18 May 2019. <https://jrupprechtlaw.com/drone-jammer-gun-defender-legal-problems#legal>
- Schnaubelt, Christopher M., Eric V. Larson, and Matthew E. Boyer. *Vulnerability Assessment Method Pocket Guide*. Washington: RAND Corp, 2014.
- Selby, William, *Small Wars Journal*, "Operating in an Era of Persistent Unmanned Aerial Surveillance." Last accessed 17 May 2019. <https://smallwarsjournal.com/jrnl/art/operating-in-an-era-of-persistent-unmanned-aerial-surveillance>
- Task Force Mali, "Op PRESENCE (MALI) ROTO 0 – End of Tour Report (ETR)" 16 Jan 19.
- United Nations, Mali. "Presence of UN Agencies and International NGO", Nations Unies, Bureau pour la coordination des affaires humanitaires (UNCHA) report. Last accessed 12 May 2019.

https://reliefweb.int/sites/reliefweb.int/files/resources/ocha_nord_presence_cercle_20160310_en_0.pdf

United States, Department of the Army, ATP 3-01.8, *Techniques for Combined Arms for Air Defense* (Washington, DC: Department of the Army, 29 July 2016).

Wallace, Ryan et al., “Exploring Commercial Counter-UAS Operations: A Case Study of the 2017 Dominican Republic Festival Presidente.” *International Journal of Aviation, Aeronautics, and Aerospace*, Vol 5 Issue 2 (J2018).

Walters, D. “Countering the Small Unmanned Aerial System Threat to the Canadian Armed Forces” *Royal Canadian Air Force Journal* 5, no. 4 (Fall 2016): 27-39.

Warrick, Joby, *The Washington Post*, “Use of weaponized drones by ISIS spurs terrorism fears.” Last modified 21 February 2017. The article also shows evidence found in propaganda video footage. https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html?noredirect=on&utm_term=.9442d1fa08de

Wendle, John, *Air & Space Magazine Smithsonian*, “The Fighting Drones of Ukraine.” Last modified Feb. 2018. <https://www.airspacemag.com/flight-today/ukraines-drones-180967708/>

Willis, Henry H. “Guiding Resource Allocations Based on Terrorism Risk,” *Risk Analysis* 27, no. 3 (2007): 597-606.

Secondary

Deneau, E.D. “Unmanned Aerial Systems Proliferation: What Does It Mean to Military Planners?” Exercise *Solo Flight*, Canadian Forces College, 2016.

Fuhrmann, Matthew and Michael C. Horowitz. “Droning On: Explaining the Proliferation of Unmanned Aerial Vehicles.” *International Organization* 71 (Spring 2017): 397-418.

Walters, D. “Countering the Emerging Small UAS Threat: The Case for a Coherent Canadian Counter-sUAS Strategy” Master of Defence Studies, Canadian Forces College, 2016.

Wong, S., R. Jassemi-Zargani and B. Kim, “Counter-Measures Against Drone Surveillance” Defence Research and Development Canada, Reference Document DRDC-RDDC-2016-D019 (May 2016).

1. CARVER TOOL

a. Topics

- (1) Criticality
- (2) Accessibility
- (3) Recovery
- (4) Vulnerability
- (5) Effect
- (6) Recognition

2. ASSESSMENT VALUES

a. Critically

CRITERIA	SCALE
Immediate halt to a CF operational role due to the loss/damage of the vital point/area	9-10
Halt to unit operation/mission within 1 day, or 66% curtailment in output, production or service	7-8
Halt to unit operation/mission within 1 week, or 33% curtailment in output, production or service	5-6
Halt to unit operation/mission within 10 days, or 10% curtailment in output, production or service	3-4
No significant effect on output, production or service	0-2

b. Accessibility

CRITERIA	SCALE
Access to the interior of the vital point/area with little difficulty	9-10
Inside the base/installation perimeter, but outside the building representing the vital point/area to within 100 meters	7-8
Inside the general base/installation perimeter but greater than 100 meters distance to the vital point/area	5-6
Inside the base/installation perimeter but at distance to the vital point/area	3-4
Not accessible without extreme difficulty; exfiltration unlikely	0-2

c. Recovery

CRITERIA	SCALE
Replacement, repair, or substitution that requires 1 month or more	9-10
Replacement, repair, or substitution that requires 1 week to 1 month	7-8
Replacement, repair, or substitution that requires 72 hours to 1 week	5-6
Replacement, repair, or substitution that requires 24 to 72 hours	3-4
Same day replacement, repair, or substitution	0-2

d. Vulnerability

CRITERIA	SCALE
Vital point/area extremely vulnerable. Offers very little or no security measures and is easily accessible from any angle. GSP ⁵³ baseline security standards are not met and upgrades are required (articulated in a current physical security survey). Emergency and security services response time exceeds 30 minutes.	9-10
Vital point/area offers minimal security measures. Although GSP standards are met, there are minor deficiencies requiring attention. Emergency and security services response time exceeds 15 minutes.	7-8
Vital point/area offers moderate security measures by meeting baseline security standards in the GSP, pursuant to a recent physical security survey. Emergency and security services response time meets the 15 minutes criterion.	5-6
Vital point/area offers substantial security measures above those stipulated in the GSP. Emergency and security response time is less than 10 minutes.	3-4
Vital point/area offers comprehensive security measures including electronic intrusion detection systems, 24/7 guards, roving patrols, overt surveillance systems, trained force protection responders (i.e. ASF/MP), comprehensive vehicle and personnel search programs, and advanced personnel identification measures within the confines of a DND establishment. Emergency and security response time is less than 15 minutes.	0-2

⁵³ Government Security Policy

e. Effect

CRITERIA	SCALE
Overwhelming negative effects	9-10
Severe negative effects	7-8
Moderate negative effects	5-6
Few significant negative effects	3-4
No significant negative effects	0-2

f. Recognition

CRITERIA	SCALE
Vital point/area is clearly recognizable under all conditions and from a distance. Requires little or no training for recognition	9-10
Vital point/area is clearly recognizable up to 500 meters and required a small amount of training for recognition.	7-8
Vital point/area is difficult to recognize at night or in bad weather and might be confused with other vital points/areas. It requires some training for recognition.	5-6
Vital point/area is difficult to recognize at night or in bad weather even under 500 meters. It is easily confused with other vital points/areas, and it requires extensive training for recognition.	3-4
The vital point/area cannot be recognized under any conditions, except by experts.	0-2

3. CARVER MATRIX ASSESSMENT

<u>UNCLASSIFIED</u>							
CAMP CASTOR (Gao)							
Vital Point/Area	C	A	R	V	E	R	Total
Personnel	6	5	9	5	10	8	42
Aircraft (Chinook & Griffon)	8	2	10	3	9	9	41
Access Control Point	7	7	6	1	7	8	36
Traffic Tower	2	3	10	2	8	8	33
Landing Area / Taxiway	3	8	2	8	2	9	32
Fuel Storage	4	1	8	3	7	6	29
Medical	3	1	8	2	8	8	30
Radar	6	1	6	1	7	7	28
Electrical Power Generation	2	1	4	1	4	6	28
Hangers	3	2	8	2	4	9	28
Communications	8	1	6	1	8	5	27
Mess/Accommodations	2	3	2	6	6	7	26
Ammo	4	1	8	1	6	5	25
Air Maintenance Bay	2	1	2	3	3	7	18

Note:

1. In the assessment of the vital point/areas, the assets were considered as a singular entity (i.e. Aircraft (Chinook & Griffon) represents the loss of one helicopter and not the full complement since the combat scenario is not peer-on-peer but rather a peacekeeping presence; therefore, it is unlikely that the opponents possess the capability to strike all the assets at the same time).
2. The result of the CARVER Matrix is used as to measure for the criticality of a vital point, and will be use to depict the likelihood in determining overall risks.

4. THREATLikelihood

CRITERIA	SCALE
Very likely to occur (91 - 100%)	9-10
Likely to occur (61 - 90%)	7-8
May occur about half of the time (41 - 60%)	5-6
Unlikely to occur (11 - 40%)	3-4
Very unlikely to occur (0 - 10%)	0-2

Probability of Threat Occurrence

<u>UNCLASSIFIED</u>						
CAMP CASTOR (Gao)						
Vital Point/Area	Threat I	Threat II	Threat III	Threat IV	Threat V	Total
Personnel	10	6	6	8	2	32
Aircraft (Chinook & Griffon)	10	5	7	4	1	27
Access Control Point	9	8	9	10	0	36
Traffic Tower	5	1	3	1	0	10
Landing Area / Taxiway	8	6	3	1	1	19
Fuel Storage	4	5	1	1	0	11
Medical	3	1	2	0	0	6
Radar	3	1	1	2	0	7
Electrical Power Generation	4	1	0	1	0	6
Hangers	5	2	2	3	0	12
Communications	2	1	1	1	0	5
Mess/Accommodations	9	6	5	6	0	26
Ammo	6	1	6	7	0	20
Air Maintenance Bay	2	2	1	1	0	6

RISK MATRIX

It is proposed to use a 5x5 risk matrix as typically used in risk management⁵⁴ and is as follows:

		IMPACT				
		Very Low (1)	Low (2)	Medium (4)	High (8)	Very High (16)
LIKELIHOOD	Very Likely (5)	5	10	20	40	80
	Likely (4)	4	8	16	32	64
	May Occur (3)	3	6	12	24	48
	Unlikely (2)	2	4	8	16	32
	Very Unlikely (1)	1	2	4	8	16

Note: The higher the number, the higher the priority.

5. PRIORITIZED ASSESSMENT OF VULNERABILITY VS THREAT

Vital Point/Area	Threat Likelihood		CARVER Score		Total
Personnel	32	L (4)	42	H (8)	32
Aircraft (Chinook & Griffon)	27	MO (3)	41	H (8)	24
Access Control Point	36	L (4)	36	M (4)	16
Traffic Tower	10	VU (1)	33	M (4)	4
Landing Area / Taxiway	19	U (2)	32	M (4)	8
Fuel Storage	11	U (2)	30	M (4)	8
Medical	6	VU (1)	28	M (4)	4
Radar	7	VU (1)	28	M (4)	4
Electrical Power Generation	6	VU (1)	28	M (4)	4
Hangers	12	U (2)	27	M (4)	8
Communications	5	VU (1)	26	M (4)	4
Mess/Accommodations	26	MO (3)	26	M (4)	12
Ammo	20	U (2)	25	M (4)	8
Air Maintenance Bay	6	VU (1)	18	L (2)	2

⁵⁴ <https://www.jisc.ac.uk/guides/risk-management/qualitative-risk-analysis>

6. NOTESa. Likelihood Scores

- (1) Items having a score between 41 and 50 are given a Very Likely (VL) rating;
- (2) Items having a score between 31 and 40 are given a Likely (L) rating;
- (3) Items having a score between 21 and 30 are given a May Occur (MO) rating;
- (4) Items having a score between 11 and 20 are given a Unlikely (U) rating;
- (5) Items having a score of 10 or below are given a Very Unlikely (VU) rating;

b. Impact Scores

- (1) Items having a score between 49 and 60 are given a Very High (VH) rating;
- (2) Items having a score between 37 and 48 are given a High (H) rating;
- (3) Items having a score between 25 and 36 are given a Medium (M) rating;
- (4) Items having a score between 13 and 24 are given a Low (L) rating;
- (5) Items having a score of 12 or below are given a Very Low (VL) rating;