AIR SPACE
ASPC's crowd-sourced blog
https://airpower.airforce.gov.au

Arnold, Chris. (2021) Air/Space Vol 2, BP16723318
Date published: 03 May 2021

Swarms of Trouble: The Hidden Threat of Consumer UAVs

Chris Arnold

There once was a time that the most dangerous thing in the air was a Sopwith Camel; slow, low flying, relatively large and easily identifiable, with ample warning of its approach. Since then things have become more complex – from the machine gun toting Camel punching at a top speed of roughly 97 knots (180km/h) we have progressed to missile-laden jets easily cruising at Mach 1.8.

Technology usually follows a certain progression – first the device gets more features before it reduces in size. And just like mobile phones started as large clunkers before becoming more powerful before finally reducing in size, so too has the ability to deliver damage to assets and infrastructure via the air and space become smaller and more bang-for-buck.

Unmanned Aerial Vehicles (UAVs) fill this description perfectly, and we have yet to come up with an adequate defence for them.

UAV, UAS, RPAS, Drones

The use of different nomenclature can cause confusion – "drones" is a general term used by professional civilian drone operators and the wider public. Search for "drone" online and small affordable eBay-type equipment is what you will find. There is a lot of overlap between the use of "UAV" and "drone", especially outside of the military.

Within international and military organisations, however, the term Remotely Piloted Aircraft Systems (RPAS) is preferred to better define aircraft that, though not having an on-board pilot, still require constant input from an operator to work. Some use Unmanned Aerial Systems (UAS) in the same context.

A reason for moving away from the general "UAV" term is to delineate civilian-type drones that have increasing amounts of automation included to help with flight such as auto-levelling and hover functions, as well as complete autonomous flight via way-points and GPS. These features remove a large part for operator input for sustained flight, making the device more autonomous and less skilfully piloted.

Wait, drones aren't new!

Remotely piloted aircraft are not unknown to the RAAF. After operating the Heron for 7 years, the RAAF has committed to acquiring MQ-4C Tritons and MQ-9B Sky Guardians through projects AIR 7000 and 7003 respectively.

The Army have also been operating UASs since 2011. Funding to projects like LAND 129 Phase 3 have resulted in a range of unmanned solutions from the PD-100 Hornet micro UAV to the 4.3 metre wide Shadow 200. DJI Phantoms have also been acquired as a trainer system to familiarise soldiers on UAS control.

Drones have even been used in warfare as far back as Vietnam. The Firebee and its descendant Lightning Bug was a Hercules-launched, jet-powered drone used for unpiloted reconnaissance missions.

Whats the problem then?

RPASs are not the issue – at least not domestically. Try transporting a MQ-9 Reaper around Sydney without getting any attention.

What does matter is small-scale UAVs – the ones readily available to consumers at a super-affordable price point. Unlike the Reaper, no-one will bat an eye at a DJI Phantom in the backseat of a car, even near airports.

But consumer UAVs are small, fast, and unpredictable. They require no airfield to deploy from and can be in and out of restricted airspace before they were ever discovered. Their radar signature is comparable to, and often mistaken for, a bird. Most radar systems disregard them because of this fact.

Detection systems do exist that can better differentiate consumer-grade UAVs, but they are not cheap and have issues of their own. Acoustic sensors have a short range and are obviously affected by loud noises as you would find on an active air base. Radio frequency sensors can detect UAVs based on their communication method back to their pilot, which means the location of the pilot can also be determined. The downside is they have no way of detecting fully-autonomous (i.e. self-flying) drones.

Prior history

Recent UAV incursions include drones appearing near nuclear power plants, international airports, and over aircraft carriers.

Palo Verde is the largest nuclear plant in the US which, over two consecutive nights in September of 2019, had a “swarm” of drones fly within close proximity of one of the cooling towers. Recent Freedom Of Information requests in the States have shown that this is not an isolated incident. From the end of 2014 to October 2019 57 occurrences of drone swarms being used over nuclear plants across the US were recorded.

A similar incursion by two drones occurred over the Gatwick International Airport over several days in December of 2018. Gatwick is the UK’s second busiest airport by passengers and, due to a combined 30 hour airspace lock down, the incident cost the airport operators over £1.4 million in lost revenue. £4 million has since been sunk into anti-UAV technology.

A separate incident in the UK saw an operator of a UAV having to report himself to military personnel guarding a docked aircraft carrier – his drone had automatically landed on the deck of the warship due to high winds.

In Australia drones are commonly used in criminal acts like dropping drugs, tech gear and other contraband over prison fences; monitoring for police presence during drug deals and meetings; and smugglers monitoring security movements and creating distractions to move illegal goods. In the case of prison contraband the Victorian Corrections department have experienced an increase in incursion reports from UAVs of over 200% in the last year alone.

So what?

Why this all matters – especially domestically and to the ADF particularly – is that the majority of our air fleet is located in Australia, on bases that are designed to keep people with malicious intent from gaining entry via the ground and, more specifically, the front gate.

Consumer-grade UAVs now provide smaller independent groups such as political/ideological groups and “lone-wolf” individuals access to cost-effective methods of causing damage to military- and nation-critical assets and infrastructure that avoids these standard defences.

By combining specific skill sets such as basic electrical engineering and computer coding abilities with the increased capabilities of low-cost off-the-shelf UAVs these groups are now better able to achieve their goals. And unlike a head-on attack via a ground access point, this kind of surprise attack can be devastating in its swiftness and overall damage.

It gets worse

Ever heard of Skyjack? Its a low-cost UAV hacking project that used off-the-shelf hobby parts, a stock DJI Phantom drone, and some open-source code to create a UAV that can take over other drones in-flight.

For those in the IT/cyberspace realms, the idea is on par with botnets – basically a control node that takes control of other nodes (in this case other drones) to create a swarm it can direct to do malicious things. Botnets are often used to attack and take down high-profile networks like the US Department of Defence. Imagine a swarm of hijacked drones that are then sent to fly into the side of a bombed-up F-35 or fully-fuelled KC-30A.

Added to the overall issue is the anonymity of UAVs – remember the Gatwick airport incident above? Cameras everywhere and yet a dedicated task force of police are yet to find the culprits. Its the same with the nuclear power plant in the US, and the only reason security knew a drone had landed on a carrier deck in the UK was because the operator asked them nicely for it back.

A printer in every home

No doubt the security of the drone operating systems will be tightened on popular consumer-sold UAVs (such as the DJI and Parrot brands) soon, but that will hardly remove the threat. Consumer 3D printing is gaining traction with the low cost, increased reliability, and more user-friendly interfaces allowing for 3D printers to become more common in modern households.

Add this to the plethora of free 3D drone models requiring everyday tools to assemble and the ease of electronic control through open-source prototyping boards such as Raspberry Pi's and a DIY drone can be built in an afternoon for less than $500, all with no complex tools or knowledge. Worryingly, unlike off-the-shelf UAVs these aren't hampered by built-in hard-coded GPS geolocation restrictions that prevent consumer drones from flying over airports.

Counting beans

That brings us round to the crutch of the problem – Return On Investment. One of the cheapest aircraft we have in our fleet currently is the PC-21 at an estimated $9m each. The most expensive will likely be the Lightning II at a very rough estimate of $220m a piece. A single decent UAV costs $1500.

Admittedly, one drone has a low probability of damaging an aircraft on its own. But what about 10? 20? That's still only $30k to put a $220m aircraft out of action for a while, possibly permanently. Accountants consider an ROI above 12% to be investment worth taking up even on the dodgiest of stocks, so even the most penny-pinching terrorist or political extremist would be hard pressed to pass up a 300% to 7,400% ROI.

You wouldn't read about it

Do you think kamikaze drones are over the top and completely unviable? You might want to mention that to the Turks. Delivery to the Turkish military of fixed and rotary wing drones (the "Alpagu" and "Kargu" respectively) is underway. These aren't just off-the-shelf UAVs with cam paint and a 400% markup; small but lethal munitions are strapped to the front to ensure that the target is receiving more than just a suicidal drone to the head.

Not surprisingly, and somewhat chillingly, they are being developed to work in a "herd" (aka swarm) to increase their effectiveness in damaging or destroying a target. Oh, and "Autonomous Intelligence" added in for that true Terminator vibe.

What can Defence do?

First, we need to look at UAV policy in Australia. The ADF has some of the most critical assets affected by this threat, and also the responsibility to protect the nation from it. The USAF Unmanned Aircraft Systems Flight Plan 2009-2047 noted that near term policy decisions must be put in place to guide development of future UAS capabilities. Though this referred to current and future system acquisitions (such as the ubiquitous MQ-1 Predator drone and its descendants), the point extends to the ADF shaping policy around systems that

pose a threat to our assets.

This means that in the short and medium term there is a need for Defence to plug in to regulators to better shape their policies regarding UAVs, especially around our bases. The Civilian Aviation Safety Authority (CASA) is the main body for this.

Policy updates for UAVs, however, are very general in nature and are quickly outstripped by advances in the abilities of new generation drones. CASA UAV rules also lump RAAF bases in the same category as any civilian airfield, affording no extra protection to airspace used by military-critical assets.

Concurrently, research must be conducted into the use of tools that can be used to protect assets on our airfields. Protection systems already exist that use different methods to bring down UAVs but they are wide-ranging in their effectiveness. From radio frequency jammers to birds of prey, they all present their own pros and cons.

A more out-there idea hand-made for Defence might include fighting fire with fire; have swarms of defence drones protecting our airfields that can detect threats further out and mitigate before they enter sensitive areas. These drones could double as normal base security and monitoring, having a set of automated eyes able to check fence lines at any time of the day or night.

Whether it be net guns, drone swarms, high-powered microwave devices, or specially trained attack birds – we must determine what will work best in protecting our assets on a base-by-base evaluation basis.

Conclusion

UAVs are fun and, for some, functional. But with every new generation the possibilities of using them effectively against our nation- and military-critical assets are increasing. Every month more innovative open-source tools are being developed by a growing group of well-meaning hobbyists and tinkerers that opens up new ways of using UAVs maliciously.

Regardless of offensive or defensive stances, when it comes to remotely piloted aircraft militarises are typically only focused on large, long-endurance systems. These are important, but the number of international incidents of small-scale UAVs (in swarms or individually) causing significant financial losses or security breaches demands an obligation to defend against similar incursions here.

We must ensure we are ready to answer the question of how we will defend against drones used in novel and malicious ways. Guiding policy is a good first step to keep normal drone operators at bay, but we need more direct systems in place to ensure we are protected against those who see an affordable solution to their malicious goals. .

Citation: text