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

Hodson, R. (2024) *Air/Space* **3**, bp41568060
Date Published: 09/09/2024

The Weaponisation of Toys and Implications for the Air Force

Ryan Hodson
Australian Defence Force

The '*poor man's air force*' is a term for employing commercial off-the-shelf (COTS) hobbyist drones or uncrewed aerial systems (UAS) to strategic level military effect, and that effect cannot be understated (Waters, 2018; Nadeau, 2022; Shift, 2023). The ability for terror organisations to coordinate multiple layers of effects, including using COTS drones, to destroy Command and Control (C2) nodes in Israel causes alarm. Couple this with the use of COTS drones for intelligence, surveillance, reconnaissance, strike and battle-damage assessment missions, and the threat posed by what are essentially toys is alarmingly real.

Many within our Defence organisation would assume COTS drones and similar are easy to counter. However, there are a number of issues presented by modern COTS drones that have soft implications across the entirety of our ability to exercise air power. The purpose of this essay is to communicate key properties of COTS drones that come into play: speed, capability, detectability, and cyber/spectrum.

Speed

COTS UAS are fast. A common COTS drone purchased from an electronics store can travel up to 60-80 kph, while a hobbyist racing drone (see **Figure 1**) can easily push 120+ kph. The world record for a racing UAS is 360.5 kph (Gross, 2024; Drone Racing League, n.d.). Even while wearing high tier Soldier Combat Ensemble, a half-kilogram toy flying half that speed presents a ballistic threat.

Figure 1. A racing drone used by the Air Force Drone Racing Association (Source: Defence Images).

UAS share a similarity to missiles. The extremes of *g*-forces that limit how fast a pilot can accelerate in a crewed jet are irrelevant to a machine. Because of this, they can get close and engage a target with very small warning times.

Capability

The hobbyist world has opened the door to innovation. However, the problem with innovation is the same as with any other facet of war, the enemy also innovates. Innovative use of UAS includes pre-programming it to identify weeds to be sprayed upon, launch tree-planting seed-pods, and heavily-lift cargo, which can all have *vastly* different applications in a military context. Modern COTS drones are extremely versatile, capable, and highly customisable.

The RPG-7 is a rocket-propelled grenade launcher that has been a stand-out in action films for decades and the advent of high explosive anti-tank RPG warheads influenced the development of modern military vehicle armour, which evolved for survivability against side-on attacks. In addition, self-protection systems such as passive infrared (IR) cameras keep an electronic eye out for launch plumes of thermal energy from a rocket being fired to trigger countermeasures. Modern tank killers, such as the US-made Javelin, exploit these evolutions by attacking them from the top, where the armour is weakest. However, by using an RPG warhead mounted on a COTS racing drone (see **Figure 2**), an operator can overcome both of these protection measures (Burgess, 2023). When delivered via a COTS drone, there is no IR plume, because no rocket was 'fired', and the drone operator can choose to attack form the top, launching a salvo at a target without necessarily exposing themselves. Most importantly, the high level of accuracy and at a significantly reduced cost per shot, presents fascinatingly barbaric considerations for the economics of war. Fleeman (2013) provides an in-depth breakdown of missile system design, including the economics (e.g. cost per shot) and calculus of such guided systems.

Figure 2. First Person View (FPV) drone carrying an anti-tank warhead (Source: Shutterstock).

This trajectory of not just using UAS for carriage of grenades or munitions, but actually *becoming* a munition itself, is a development trajectory that has been shared by defence industry. Before the Ukraine-Russia war, there were limited offers for the 'loitering munition' style of system, which can be: directed to terminal effect, optionally disarmed and sent back to recharge, or used to send a satchel of blood and medicine, a radio, or ammunition to a frontline combatant. There are now however considerably more options available directly on the market – the innovative development of new methods to generate effects has essentially given rise to a new military off-the-shelf (MOTS) UAS, the loitering munition/tactical missile.

Detectability

Drones are small, but their exact size is not defined. You could say most drones are approximately *yay-big* and make a rough hand gesture, but the reality is it depends a lot on the type, class and intended purpose of a drone as to their size. For example, the Black Hornet 3 is not equivalent to an MQ-4C Triton. Most COTS drone toys will probably fall into the *yay-big* category, around the Type-2 mark, or very small to small category in accordance with Part 101 – Unmanned aircraft and rockets of the *Civil Aviation Act 1988*, but this is still soft terminology.

UAS can operate in complex urban environments, and depending on the type and their configuration, they can hover, glide, or thermal like a bird. Further, an Australian company, Sypaq, is shipping drones to the Ukrainian war effort that are made out of cardboard (Sypaq, 2024).In comparison, a Lockheed Martin F-35 Lightning II is made mainly of titanium, has a standard shape, and broadly speaking has a standard set of speeds it operates within. The importance of these differences in properties is apparent when considering our default detection option for airborne threats: the radar. It becomes more complex to determine what is a drone and what is not when we have to consider a wide variety of sizes, shapes, speed, and materials. Most importantly, it becomes more difficult to identify if the target is just one drone or multiple, and as such the radar used for this detection purpose must be quite advanced.

The end state is not one standalone system but multiply coupled systems, typically including a radar with an electro-optics, IR or thermal imaging suite, an acoustic sensor suite, and even a signals detection suite. All systems provide more information and essentially be able to provide basic answers to: *is it a drone? Or is it a threat?*

Cyber and Spectrum

Organisationally, cyber offensive/defensive warfare, electronic warfare, and electromagnetic spectrum warfare and manoeuvre, are considered part of the Cyber Domain enterprise. However, it is worth considering them independently in this article. Adamy (2015) provides an extremely succinct approach to considering them both separately and conjoined.

The cyber impost from COTS UAS is not just figuring out how to 'hack' the 'enemy drone'. A UAS can be both the receiver and the bearer of a cyber effect or payload. The drone does not necessarily have to carry a bomb to be a threat. It can carry a low-power jammer, or a custom radio kit to skim mobile phone data. Similarly, a drone's detectability as discussed earlier invokes cyber equities especially when we deploy a number of standalone systems that are performing different elements of the *find-fix-finish*[1] engagement sequence. For the drone detectors to be truly effective or modernised, they need to be interconnected to a central node and share real-time data. This means that the cyber-attack surface grows as these standalone systems, which are notoriously bad for talking to each other to begin with, are integrated.

Radiofrequency spectrum ends up being a similarly flavoured dialogue. For effective use of detection systems, you generally need wide bandwidth systems with aggressive pulse interrogation methods and low spectral occupancy, which is a steep requirement given the value of spectrum in the modern day. Most radar products end up being multi-band, such as *L*- or *S*-band volumetric search radar and *C*- or *X*-band target classification radar, increasing the impost across different segments of spectrum, leading to trade-offs in use or functions. And for truly deployable systems, you need data-link type systems so that there is no need to run a spool of fibre-optic cable all over the base.

---

[1] In classical air power doctrine, the engagement sequence for identifying a threat and essentially doing something about that threat is: Find, Fix, Target, Track, Engage, Assess (F2T2EA). The simplified sequence is to Find, Fix, and Finish a target – often referenced as a quicker and alliterative alternative to the full sequence.

So far, this discussion has been centred on detection mechanisms – the *find* and *fix* of the simplified engagement sequence. From an effects[2] basis (‘*finish*’), there are many who would point to radiofrequency jammers as the one-size-fits-all solution. But to effectively counter COTS UAS, you need to jam the multiple frequencies they operate on in addition to radionavigation satellite services, such as global positioning systems (GPS). MOTS jammers will also almost certainly have unintended emissions. You might jam the target, but you might also jam your own radar that is detecting the target. This could be an acceptable trade-off if considered, however if not part of a deliberate course of action this instead causes confusion. The other difficulty is that spectrum does not respect boundaries – turning on a jammer at the Russell offices in Canberra may sound fine, until the azimuth of the jammer is pointed towards incoming civil air traffic whose primary source of air navigation, GPS, is now denied.

What’s the *So-What*?

Many COTS and MOTS detection products argue detection ranges measured out to 10 km as an upper bound[3]. That means, best-case scenario with ideal conditions, the furthest we can see an OPFOR drone is around that 10 km mark. The speed and detectability of COTS UAS translates directly to time until the target arrives, as shown in **Table 1**.

Distance (km)	Time to target (minutes) at different UAS speed (kph)				
	60 kph	80 kph	120 kph	160 kph	200 kph
15	15	11.25	7.5	5.6	4.5
10	**10**	**7.5**	5	3.75	3
5	5	3.75	2.5	1.9	1.5
2.5	2.5	1.9	1.25	0.9	0.75
1.5	1.5	1.1	0.75	0.57	0.45

Table 1. The time (**minutes)** for a UAS travelling at a given speed and from a distance to arrive at a target. Note that COTS drones have approximated maximum speeds of 60-80 kph, with MOTS CUAS radar operating typically out to 10km given ideal conditions.

What this means is that the window to determine a course of action, to inform superiors, seek clarification (if required), assess extant SOPs, and then pull a proverbial trigger is measured in *minutes*. An operator, therefore, may not have time to consider multiple information feeds, such as radar track, imagery, acoustics and signals, which are best delivered in one interface, or better yet, pre-analysed with machine-learning analytics to provide a classification of system and any associated history. The *find*/*fix* system has to act quickly, autonomously, and the operator has to trust the outputs, because they simply may not have time to double-check or confirm response options.

Trust is a funny thing to consider, because trust is built and established over time, and the reality is that the technological landscape is changing faster than we are. Trust, in the traditional concept then, has to be generated from first principles. Our aviators must be broadly educated to understand fundamentally how modern drones will be employed against them,

[2] The consideration of an effects basis of a detection function could legitimately become an essay of its own right and is beyond scope here. Consider the trade-off between use of radar spectrum to perform a search function versus the use of that same spectrum by telecommunications companies to provide a government mandated warning to the civil population of an inbound lethal threat.

[3] Anecdotally based on a review of most 5EYES MOTS products. A quick walkthrough of the Land Forces or Airshow series, and a review of trade show exhibitions therein, will quickly demonstrate this number. As discussed for detectability, it is hard for many companies to put a definitive number to this without qualifying the specific size (type), shape and/or material – most will measure against a DJI Mavic 3 or similar.

and therefore how our defensive measures work on their behalf. Speed, therefore, is not just a threat in its own right in terms of *how fast that thing is coming my direction,* but also an artefact of the pace of change we are experiencing – the speed of innovation and evolution.

The "*So-what?*" is that COTS small UAS are not only a threat, they are hard to counter effectively, and the impacts of this flow throughout our ability to generate air-power. Soft-kill methods to attack UAS, including jammers and cyber effects, are only effective so long as you're ahead of the technology evolution cycle – and the adversary has a say in how they pursue innovation – whereas hard-kill methods are extremely effective but unlikely to be seen around Australian bases[4]. The *poor man's air force* of strapping rifle grenades and RPG-7 warheads to a first-person view drone has changed our own decision-making calculus for security effects and air power. This is not a paradigm shift, where an adversary might suddenly create a new military power offset. This is a soft impact that ripples gently throughout our air domain ecosystem.

Our ability to provide security effects is impinged by urban encroachment. Legitimate and illegitimate drone users can come closer to our domestic security boundaries, reducing the time to identify and react to them. The security of that close airspace is threatened; nuisance (accidental and on purpose) UAS flights within safety-critical volumes of approach and takeoff vectors already occur. The ability to identify targets and prosecute an effect is challenged by 5G/6G encroachment and poaching of our vital radar spectrum, and by perceived and actual issues in legal/doctrinal frameworks[5], and further issues associated with effects-based capability rollout. How quickly the threat landscape has changed highlights how slow we can be to respond to this.

Conclusion

Domestically, we are still fundamentally safe, but we cannot ignore the impact of the *poor man's air force*. Future adversaries will almost certainly seek to exploit similar techniques as Hamas did in Israel, seeking to saturate air defence networks with high numbers of attritable systems in order to increase the likelihood of success for a sophisticated capability. In a first-wave attack, these could be as simple as anti-radiation loitering munitions, which would *find, fix* and *finish* high power emitters like jammers, radar or directed energy weapons – this widens the offset to allow further SEAD capabilities. A smart adversary will not necessarily risk their tombstone[6] platforms or capabilities in a first strike, especially when they can just as easily field cheap toys for a degrading effect first.

It is worth considering that the above represents a peer warfighting scenario. COTS UAS present a threat, and although they are being used in multiple theatres, this does not necessarily invoke a paradigm shift for the RAAF on any *fundamental* level. Understanding

---

[4] Deployment of CIWS or 25mm air-burst autocannons and similar is unlikely to be seen as favourable by the public in locations already encroached by private housing, such as RAAF Amberley, RAAF Williamtown or RAAF Edinburgh.

[5] Perceived or actual gaps or issues in doctrine, to the exclusion of perceived/actual issues in legal frameworks, could fill an additional text, and have not been covered here in order to approximately remain true to a word count. However, the key message is this: where perceived or actual conflicts in doctrine or law exist, they create points of indecision for commanders and subordinates, and that indecision costs time – a vitally precious resource.

[6] Author's note: unfortunately, I am unable to find the specific *Association of Old Crows* journal article that discussed the centralisation of key warfighting power as being 'tombstones' of the central fighting axis. However, the key takeaway is that the primary capabilities of traditional warfighting domains – tanks, aircraft carriers/air warfare destroyers, and strike aircraft – were in Western military doctrine considered the tombstones; the fundamental weight behind the strategic mass of a battlespace engagement. In considering *first strike capabilities*, the tombstone assets are likely to be low-probability of detection long-range hypersonic missiles – the exquisite, the few, and the utterly devastating capabilities designed to inflict maximum damage in order to shape the only possible end state of the war at day 0.

and educating our aviators as to the scheme of modern threats, recognising their impacts across our capabilities including impacts to cyber, spectrum, and personnel, will go a long way towards understanding these threats as we explore further systems to defeat them across the entire continuum of conflict.

Our ability to project air power at the enterprise level is still impacted. We can be challenged by toys, but that is due primarily to the convergence of a diaspora of problems they present. If we can solve those challenges, educate and uplift the entirety of our working force, we will be in a better position to pivot at the *next* challenge.

References

Burgess, A. (2023, April 1). *Why Ukraine's kamikaze racing drones are causing a buzz on and off the battlefield*. Retrieved from ABC News: https://www.abc.net.au/news/2023-04-01/fpv-racing-drone-kamikaze-attacks-ukraine-russia-war/102155702

Fleeman, E. L. (2013). *Missile design and systems engineering.* American Inst of Aeronautics & Ast. doi: https://doi.org/10.2514/4.869082

Gross, R. (2024, March 9). *5 Fastest Drones in The World Including Guinness Record Holder*. Retrieved from Propel: https://www.propelrc.com/worlds-fastest-drones/

Drone Racing League (n.d.). *179.78 MPH Speed Machine: DRL RacerX: Fastest drone in the world*. Retrieved from Drone Racing League https://www.drl.io/racerx

Nadeau, M. (2022, March 27). *Drone Wars: The Poor Man's Air Force*. Retrieved from BookMarc: https://bookmarc.ca/2022/03/27/drone-wars-the-poor-mans-air-force/

Shift, D. (2023). *Poor man's Air Force: A guide to how small drones might be used in domestic unrest or low intensity conflicts,.* Independently Published.

Sypaq. (2024). *Corvo Aytonomous Systems*. Retrieved from Sypaq: https://www.sypaq.com.au/solution/corvo-unmanned-systems/

Waters, N. (2018, January 18). *The Poor Man's Air Force? Rebel Drones Attack Russia's Airbase in Syria*. Retrieved from bellingcat: https://www.bellingcat.com/news/mena/2018/01/12/the_poor_mans_airforce/