Centre for
Risk Studies

UNIVERSITY OF CAMBRIDGE
Judge Business School

McKinsey & Company

Cambridge - McKinsey Risk Prize Bio-sketch and Photo Page

Student name: Vito Cientanni

Email contact vc329@cam.ac.uk

Date of submission: 3rd April 2023

Title of submission: Vulnerabilities to national security from low-cost unmanned aerial vehicles

I am a candidate for the degree: DPhil

Department: Department of Engineering

Linkedin profile link: https://www.linkedin.com/in/vito-cientanni/

Biosketch (approximately 150 words)

Vito Cientanni is a PhD candidate in the Department of Engineering, working within the Bulk Superconductivity Group using numerical methods for analysing the thermal and magnetic properties of bulk superconductors, with a focus on thermomagnetic instabilities. A recent paper that Vito published is on the techniques for modelling and mitigating flux jumps in bulk high-temperature superconductors, and can be found at: 10.1088/1361-6668/acaa06. Vito has a keen interest in UAV technology, and has developed over 7 different low-cost and accessible UAV platforms as an extracurricular activity, providing designs and systems for the hobbyist & academic community.

Centre for
Risk Studies
UNIVERSITY OF CAMBRIDGE
Judge Business School

McKinsey & Company

Cambridge - McKinsey Risk Prize

Declaration Form

Student name: Vito Cientanni

Email contact: vc329@cam.ac.uk

Date of submission: 3rd April 2023

Title of submission: Vulnerabilities to national security from low-cost unmanned aerial vehicles

Number of words of submission: 6151 words

I am a candidate for the degree: PhD

Academic Institution/Department: Department of Engineering

Declaration

I confirm that this piece of work is my own and does not violate the University of Cambridge Judge Business School's guidelines on Plagiarism.

I agree that my submission will be available as an internal document for members of both Cambridge Judge Business School and McKinsey & Co's Global Risk Practice.

If my submission either wins or receives an honourable mention for the Risk Prize, then I agree that (a) I will provide a recorded 2 minute overview of my paper, (b) my submission can be made public on a Cambridge Judge Business School and/or McKinsey & Co websites.

This submission on risk management does not exceed 10 pages.

Signed (Electronic Signature)

Please include this declaration form after the cover page of your paper submission.

Vulnerabilities to national security from low-cost unmanned aerial vehicles

Introduction

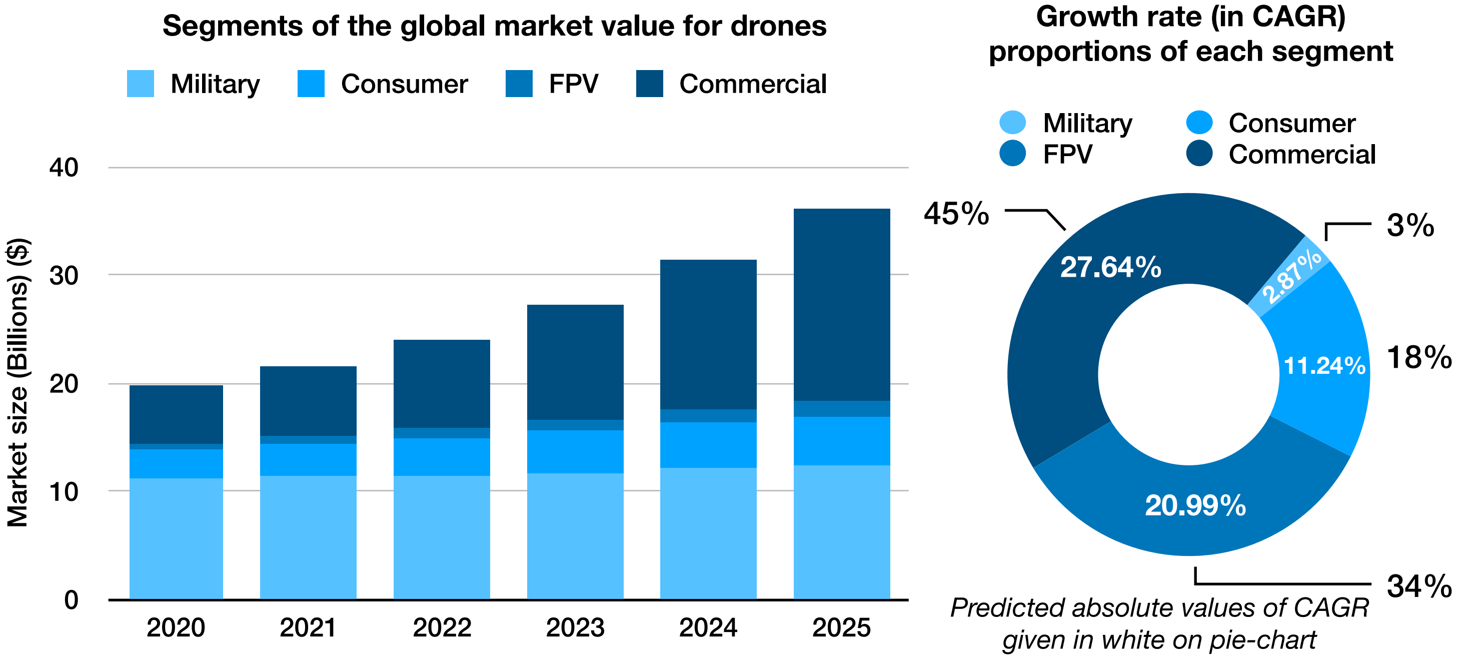
Unmanned aerial vehicles (UAVs, or drones) are firmly set to revolutionise the way consumers interact with the world; from medical supply deliveries in Rwanda [1], to the ambitious spurs of flying taxi startups [2, 3], it is clear UAVs should help to define the next 50 years of global trade and transport. Despite their promise, industry regulation is still premature, and in truth, quite rightly. Commercial aircraft are expected to critically fail no less than once every billion hours of flight, an unrealistic demand of an industry undergoing rapid transformative technological change year-to-year [4].

However, this very lack of regulation (but also, a severe lack of effective technology) exposes a vulnerability to attacks on infrastructure and civilians using these devices. We've seen throughout the Ukraine the extent of damage possible with a drone and a hand-grade [5], yet also close to home, an estimated £54 million was lost over two days at Gatwick airport due to suspected drone flights; with no culprit ever found [6]. These devices are therefore not only capable of significant disruption and damage, but they are also highly accessible, costing as little as $400 for a state-of-the-art consumer drone [7]. We must therefore ask, how do we protect ourselves from attacks using drones, and what (or who) in our society is most vulnerable to such an attack? We explore in this investigation exactly what could go wrong when malice and drones are combined, if anything can be done to stop it, and imagine the doomsday scenario of just how bad this threat could really be.

Section 1: Identifying risks from UAVs

It would be useful to first clarify the scope of the term 'drone', defining what types of risk they may present, and to who. We can broadly segment drones by their different end-users; the military, consumers, commercial users, and finally 'FPV' users (or first-person video). Military drones include the perhaps familiar 'Predator' drone, first made infamous during the Iraqi war [8]. Drones in this class are very high cost, highly sophisticated, and inaccessible to the general public. Indeed, the average cost per unit globally for this type of drone is $2.5 million, and despite their devastating potential, they are not the focus of risk in this essay. Instead, we focus on the latter three; 'consumer', 'commercial' and also 'FPV' drones. Consumer and commercial drones are broadly the same in that they are intended for non-specialist pilots with high ease-of-use, usually operating with some level of autonomy. Drones in these categories generally focus on photographic, videographic, and surveillance functionality, combing professional camera equipment with reasonable flight-times [9]. The speed and range of these drones are generally limited, not just technologically, but also with established regulation from bodies such as the CAA and the FAA [10]. Commercial drones are expected to have a market value of over $17.7 billion by 2025, with an average CAGR of 27%, becoming the largest sector of the drone market, and the fastest growing (see figure 1 & 2).

Figures 1 & 2



Segments of the global market value for drones

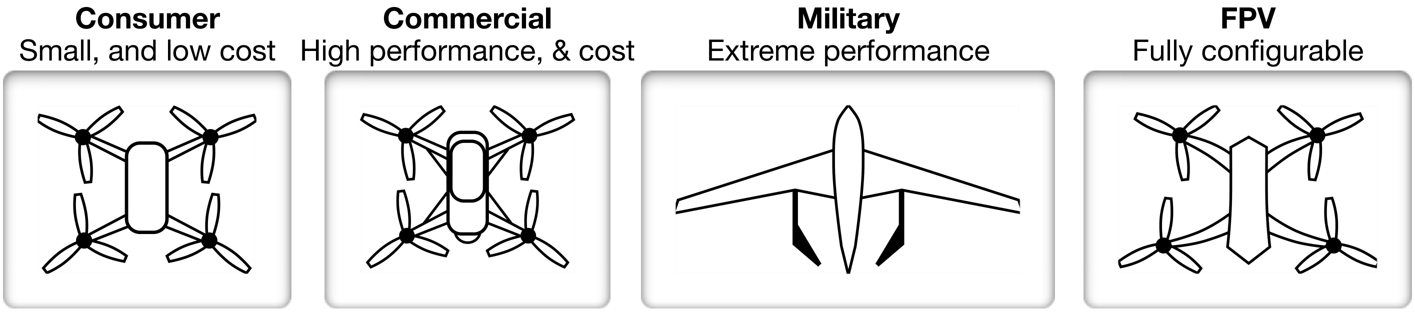
Growth rate (in CAGR) proportions of each segment

Predicted absolute values of CAGR given in white on pie-chart

Data gathered from the following sources; Polaris Market Research, Teal Group, Stockholm International Peace Research Institute, Fortune Market Research, and Statista.

Finally there is a small but fast growing area of drones; the FPV drone [11]. An FPV, or first-person video drone, can be made of essentially any material, be any design, and have any purpose. They are a mix of home-made constructions developed by an enthusiast, or ‘ready-to-fly’ models made by a small firm with low-volume manufacturing techniques. The fast growth is due to both their extreme performance capabilities and the increasingly low cost technological advancements, enabling simple and modular construction or augmentation. Figure 3 below illustrates some of the basic features of these different drone types, where from herein the three groups ‘consumer’, ‘commercial’, and ‘FPV’ will be referred to as ‘civilian’ drones. When focussing on the risks that these drones may present, it’s therefore natural to consider both national and public security. That is, risks to the general public and the wider nation due to malicious intent applied using these types drones.

Figure 3



Consumer
Small, and low cost

Commercial
High performance, & cost

Military
Extreme performance

FPV
Fully configurable

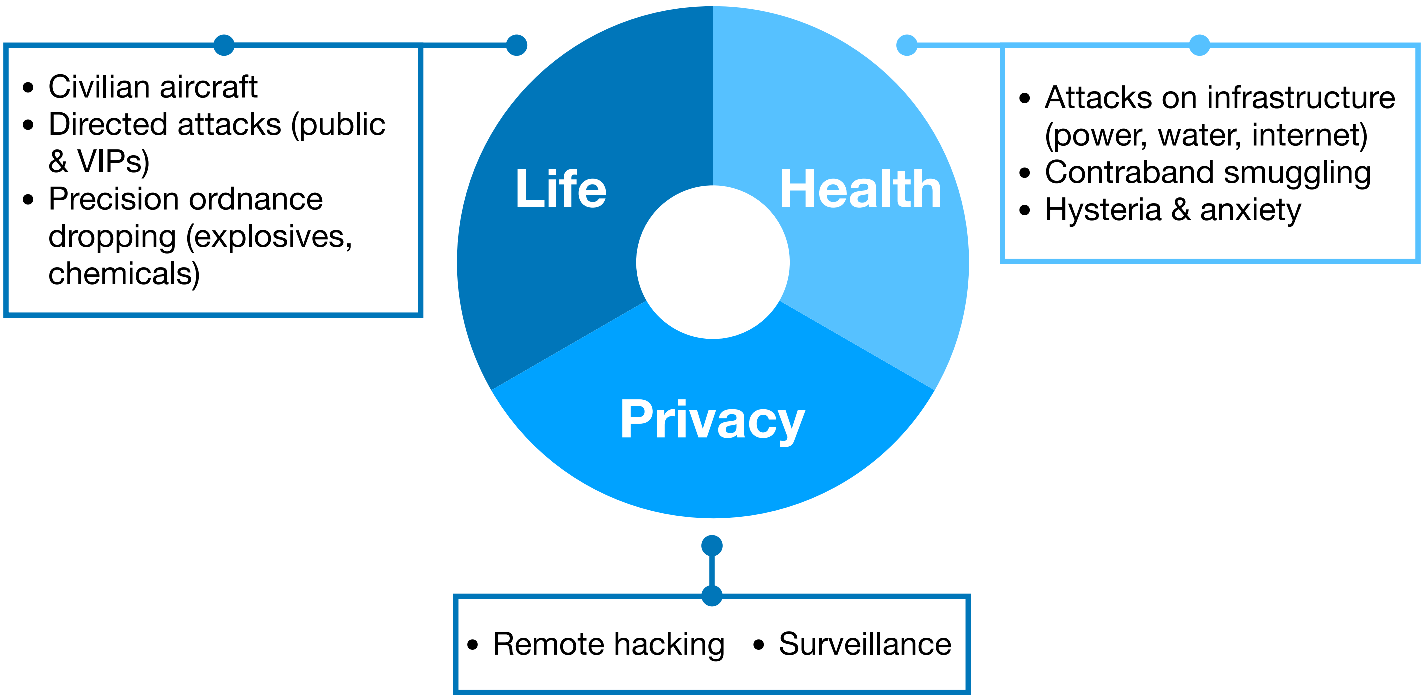
	Consumer	Commercial	Military	FPV
Price/unit (dollars)	**$540**	**$1500 - $30,000**	**$2.5 million**	**$60 to $1000**
Accessibility	**High**	**Medium**	**Very low**	**High**
Size (meters)	**0.15 - 0.35**	**0.3 - 1.5**	**0.1 - 20**	**0.1 - 1.5**
Flight time (hours)	**0.12 - 0.5**	**0.25 - 2**	**0.25 - 50+**	**0.05 - 2+**
Range (km)	**0.1 - 10**	**0.1 - 200+**	**0.1 - 200+**	**0.1 - 200+**

Estimated by averaging the price of the top 12 best selling consumer drones from top 3 companies, top 7 are from DJI. Price ranges significantly depending on customisation and options, the lowest level considered is a DJI Mavic. Military estimate from the 2023 world wide (published) units of military drones in service and the overall contract value of global military drone spending (Teal group, Stockholm International Peace Research Inst.). FPV estimated from low range (BetaFPV Cetus) and high range (MrSteele Apex 5” with additional camera drones). Accessibility estimated by assessing ease of purchase (i.e. distribution) and cost. Flight time can vary dramatically based on design, including use of gasoline power or fixed wing (over multi-rotor) design. Some military drones are capable of providing/being mid-air refuelled, significantly increasing time in air (and range). Range depends strongly on design; radio controlled can have ranges in excess of 12-15 km (with some FPV home-made designs even larger), but 4G-technology and SPL (satellite control) can make range effectively global.

With the drone type and those at risk chosen as the focus, we can examine what kind of risks ‘civilian’ drones may present to the public. We can divide the risks from ‘civilian’ drones into three categories, as seen in figure 4; risks to life, to health, and to privacy. Risks to life may be the most serious category in figure 4, where small civilian drones can be used to either kamikaze attack (i.e. flying at speed into the chosen target, with-or-without ordnance), or to drop ordnance, often with high precision, at altitude over the target. We have seen both of these types of attacks in the Ukrainian war; in particular from the Ukrainian army using the flexibility and high speed of FPV type drones to destroy tanks [12], armoured personnel vehicles, or trenches. Additionally, consumer drones (such as the DJI Mavic) have been used with a modified, low-weight grenade, to hover silently above targets before dropping an explosive [13]. Interestingly, considering wars are won and lost by the strength of the economy backing them, this has a scenario where drones costing less than $1000 can readily destroy $3 million tanks [14]. This further raises the question; who else might be able to utilise these highly accessible drones, and what else would they be able to destroy?

Figure 4

Various risks from civilian drones


Life
Health
Privacy
• Civilian aircraft
• Directed attacks (public & VIPs)
• Precision ordnance dropping (explosives, chemicals)
• Attacks on infrastructure (power, water, internet)
• Contraband smuggling
• Hysteria & anxiety
• Remote hacking
• Surveillance

Such drones could also be utilised in similar ways to attack infrastructure (through destructive means, or by serving as a remote access hacking station). Real examples of these types of risks from the past couple of years include:

- A drone discovered after unsuccessfully attempting to ‘short-circuit’ a national grid transformer with a large copper cable [15].
- Submarine drones discovered during a targeted raid on a drug smuggling gang in Spain, capable of transporting over 200 kg of contraband each [16].
- Mexican cartels found using an array of drones to perform smuggling operations [17].
- Additionally, a large study conducted in Afghanistan investigating anxiety and the psychological impact of drone use on the civilian population, finding they have caused mass trauma [18].

Finally, drones may present a significant risk to privacy, both to corporations and to the general civilian population. Both remote hacking and surveillance have been demonstrated as dangers of civilian drones in the wrong hands, including:

- Two drones found snooping on a financial institution with ‘pineapple’ devices (a type of Wi-Fi eavesdropper) [19].
- US law enforcement agencies have been found controversially using aerial drone surveillance to obtain evidence without warrants [20].

As mentioned, the risks to life category is arguably one of the most severe risks that these drones could present, and next we will analyse these risks in particular. Examining this threat in the U.K., used an example western nation, two possible scenarios that could happen tomorrow are analysed below.

Section 2: High-risk scenarios

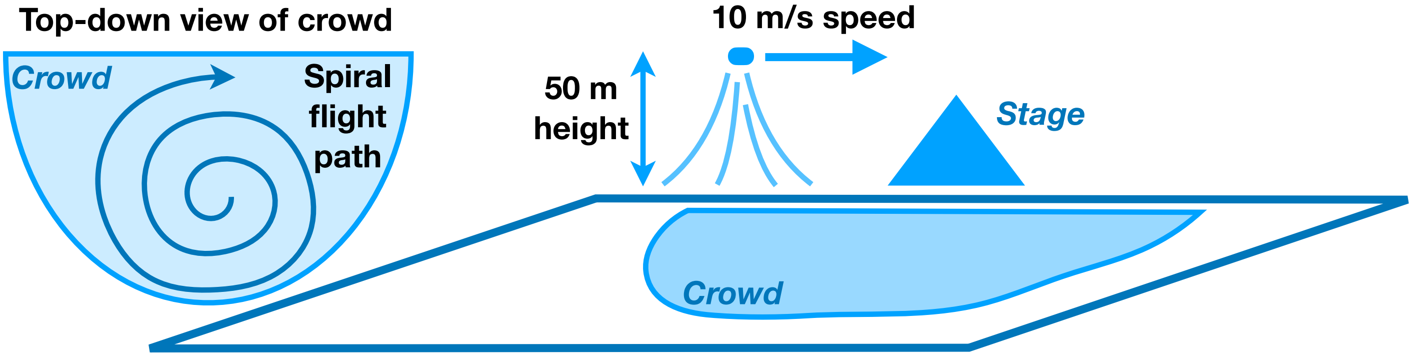
The first scenario analysed is that of an ordnance drop, specifically the dropping of a chemical nerve agent via an agricultural crop-spraying drone. In the commercial class of drones, agricultural drones have enabled famers to apply agricultural chemicals to their crops, with rapid speed, and high accuracy. They can often work autonomously, and even in networked swarms, increasing productive efficiency in the farm [21]. Most of these drones are over a few meters large, with payloads of 10 or more litres of chemicals, however some low-cost solutions such as the Skykrafts Kisan (which is the world’s smallest spraying drone), can cary a modest 0.5 litre payload and is less than 40 cm wide. It can be remotely operated from up to 5 km away, has a flight time of 15 minutes, and can fly autonomously at 22 mph (but well over 100 mph in manual mode, with failsafes disabled) [22].

Whilst these devices have been designed to disperse agricultural chemicals, which usually have properties close to that of water, any dangerous chemical with similar viscosity and density could be efficiently dispersed using these systems (with little-to-no modification). Nerve agents such as Novichok and VX, are some of the most deadly and potent nerve agents created by man, and happen to share this property making them suitable candidates for a nerve agent attack using an agricultural drone. Indeed, with its 0.5 litre payload capacity, the Kisan would be able to store over 50,000 deadly doses of VX nerve agent in a single flight, and with four spraying nozzles situated under each propeller for maximum dispersal, it can disperse the chemical at a rate of 200 deadly doses per second [23]. This means that attacks such as those on Kim Jong-Nam in Kuala Lumpur International Airport in 2017 [24], and the 2018 attack on Sergei and Yulia Skripal in Salisbury, UK [25], could be conducted remotely, autonomously, and over very large areas affecting thousands of people within seconds. Considering the modest size of the Kisan, it could even be retrofitted with modern low-noise propellers to be significantly quieter [26], which could make it much harder to detect both visually and audibly. With the speed and size of the application, in the worst case scenario, a single one of these drones could fly a pre-programmed path around a metropolitan area dispensing deadly nerve agents at a terrifying rate.

Having outlined the risk above, we can now analyse the potential impact of such a scenario applied to a real-life place and event. Such an event could be a musical festival, which in the UK is a $2.15 billion business, with nearly 1000 festivals held per year [27]. Some of the largest festivals can host over 200,000 attendants, over multiple days, generally in open fields. Figure 5 illustrates diagrammatically how such an attack could be planned at a festival, and describes the analysis performed to estimate the impact. Using the Kisan agricultural drone for it's small size and hence low visibility at height, with a full payload of 500 ml of VX nerve agent, it is estimated that over 33,000 civilians could be injured or killed within 25 minutes of launch, potentially without anyone discovering the drone at all. The cost of damage to this attack, would be at minimum $147 million per year if such a festival were cancelled, but likely much more due to the sheer loss of life. This is an incredibly devastating attack, and as we shall investigate later, there is very little in the way of effective countermeasures to prevent such an attack from occurring (even if the drone is seen during the attack).

Figure 5

Schematic of hypothetical attack on a festival



Potential fatalities	Potential economic loss
33,000	$147 million

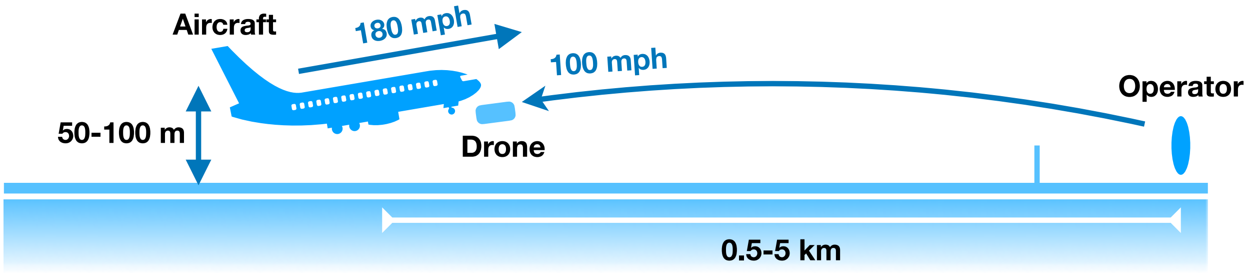
Estimated casualties: calculated by assuming a crowd of 80,000 attendees, with a flight of 10 minutes at 10 m/s, flown in a spiral path with a maximum diameter of approx. 0.5 km. Dispersing at a rate of 50 ml of VX per minute, this would cover an area of approximately 0.18 km^2 (assuming 4 loops of a spiral). Assuming a density of 1 person per m^2, a 50 m flight altitude, and doses spread horizontally by approximately 1 m for every 5 m fallen, the deadly dosage falls to 0.83 per m^2. Hence assuming that 0.83 of a dose correlates to a 83% chance of death, and also a further 50% survival rate, the total fatalities are 33,200.
Estimated damages: calculated by assuming the total revenue of a festival is from a £300 average ticket price, and 200k attendees, contributing the cost of the festival cancellation, but then also that there is a doubling of GDP loss due to the multiplier effect on the local economy from the festival. An exchange rate of £1 to $1.22 was assumed. This loss likely to be much greater considering the sheer magnitude of fatalities that could occur due to this attack.

Despite the estimated economic impact and potential fatalities in this scenario, the assigned risk by the author is ranked lower than the second scenario analysed below. This is mercifully thanks to the inaccessibility of these compounds, as only very limited quantities can be legally produced by research institutions, and they are not easy to create without specialist knowledge [28].

In the next scenario, a different type of drone is considered, the FPV drone. As mentioned, these have seen rising popularity due to their low cost, increasing ease of use and assembly, and the high performance these drones can offer. Most users of these drones are hobbyists, who enjoy the experience of flying acrobatic drones. These types of drones can be classed as either multi rotor (utilising fast spinning propellers to generate lift, similar to a helicopter), or as fixed wing drones (utilising aerofoils and wings to generate lift, similar to a plane). The ability of these drones greatly depends on the design and purpose; some have very long range and flight time (usually fixed-wing), and others can fly briefly at incredible speeds and accelerations (usually quad-copters, a multi-rotor with four motors). It is this second type of drone, the quad-copter, which has found significant popularity over the past decade, with many options for an FPV hobbyist to create a drone fitting their exact preferences. A typical quad-copter with 5-inch propellers and a powerful battery could be expected to fly around 5-10 minutes, and accelerate from 0 to 100 mph within 2 seconds, with a low-end cost of approximately $350 [29].

The next scenario we consider is the risk exposed to commercial airliners from this type of drone. Studies have investigated the risk that a consumer or commercial drone (comprising mostly fragile plastic) poses to aircraft. It has been shown they can pose a serious threat exceeding current civil aviation certification [30, 31]. FPV drones however are extraordinarily durable due to their high performance, and are almost always constructed with strong carbon-fibre and metal frames. They are designed to survive impacts at speeds in excess of 100 mph, and hence the risk of damage to a commercial aircraft from these drones could be significantly higher than previous studies have shown. An important thing to note about these types of drones is they utilise large and powerful lithium polymer (or LiPo) batteries, which can be relatively unstable. If pierced or damaged, a 'LiPo fire' can produce a sustained flame at temperatures in excess of 1500ºC [32]. It is likely these batteries would be sufficiently compromised in a collision with a commercial aircraft, especially if flown into the turbofan engine intake. Figure 6 outlines a possible attack.

Figure 6 **Schematic of potential aircraft attack**



Potential fatalities	Potential economic loss
185	$540 million

Estimated casualties: calculated by assuming the average seat capacity of a commercial airliner is 350 seats, with average occupancy of 85%, and a crew of 6, and also a survivability of the crash at 60% (considering the lower speed and altitude), including approximately 5 grounded civilians who may be killed during the crash.
Estimated damages: calculated by summing the average cost of a commercial airliner assumed as $250 million, an estimated damages of $20 million to infrastructure and property, and the economic impact of the resulting closure of the surrounding airports throughout investigation (assumed as 3 days of closure of 3 main London airports, and an estimated $30 million per day per airport).

This scenario, where a FPV drone is intentionally flown into the engine intake of a commercial aircraft, could be realised during the landing or take-off phase close to an airport. Whilst no-fly geo-fences would prevent many consumer drones from being able to fly here, an FPV drone has no such prohibitive function, and indeed there is no hardware or software limitation to where and how they are flown [33]. If an operator with malicious intent situated themselves close to an airport, within 5 km perhaps, it would be possible to fly the drone head-on with a collision velocity in excess of 280 mph into the turbofan engine. Whilst usually capable of surviving accidental ingestion of birds (which are relatively soft), a fully carbon fibre and metal drone would likely cause significant structural damage [30]. In particular, if the LiPo battery remains in the engine whilst it becomes damaged, the sustained high-temperature fire could create a risk of ignition of the fuel (depending on extent of structural damage). The most pressing issue however, is that even if the aircraft remains structurally intact, with a failed engine at take-off speeds, the aircraft will quickly lose altitude and likely stall (i.e. fall from the sky). If this happens during take-off as the aircraft passes the end of the runway, there are very little options for the pilot, and it will likely result in a serious crash of the aircraft. It is estimated approximately 185 people could die in such an attack, with an economic cost of over $500 million in the first few days after the attack. This number would likely increase significantly with time due to the reduced confidence in aircraft transport, and other factors (such as the cost of the ensuing investigation). This scenario has been ranked highest in risk, due to the very high accessibility and low cost of the implements required to enact such an attack, and further because of our current technological inability to stop such an attack occurring. Even though it could be possible to detect this drone at an airport with current technology (as examined in the following section), if it takes off within 500 m of the aircraft it could arrive at the target within 4 seconds of the drone take-off, at the collision velocity of 280 mph. Such a short period of time leaves effectively no chance for an effective human response.

Section 3: Countermeasures

Having outlined the potential risks and two potential types of attacks that could be made using this technology, we analyse current anti-drone systems and countermeasures, identifying how many fail to effectively counter certain drones. Counter-drone technology, or C-UAS is a growing industry due to the rising risks these devices present, expected to grow at over 20% CAGR by 2030, and valued last year at over $0.6 billion [34]. Counter-drone systems must first utilise drone detection methods, and then if needed, use drone countermeasure methods. Drone detection and sensing involves either analysing frequencies (emitted by the drone or the operator), or through using imaging & reflection (radar) techniques.

Types of drone detection

Frequency analysis

- **Radio Frequency detection**
- **Acoustic detection**

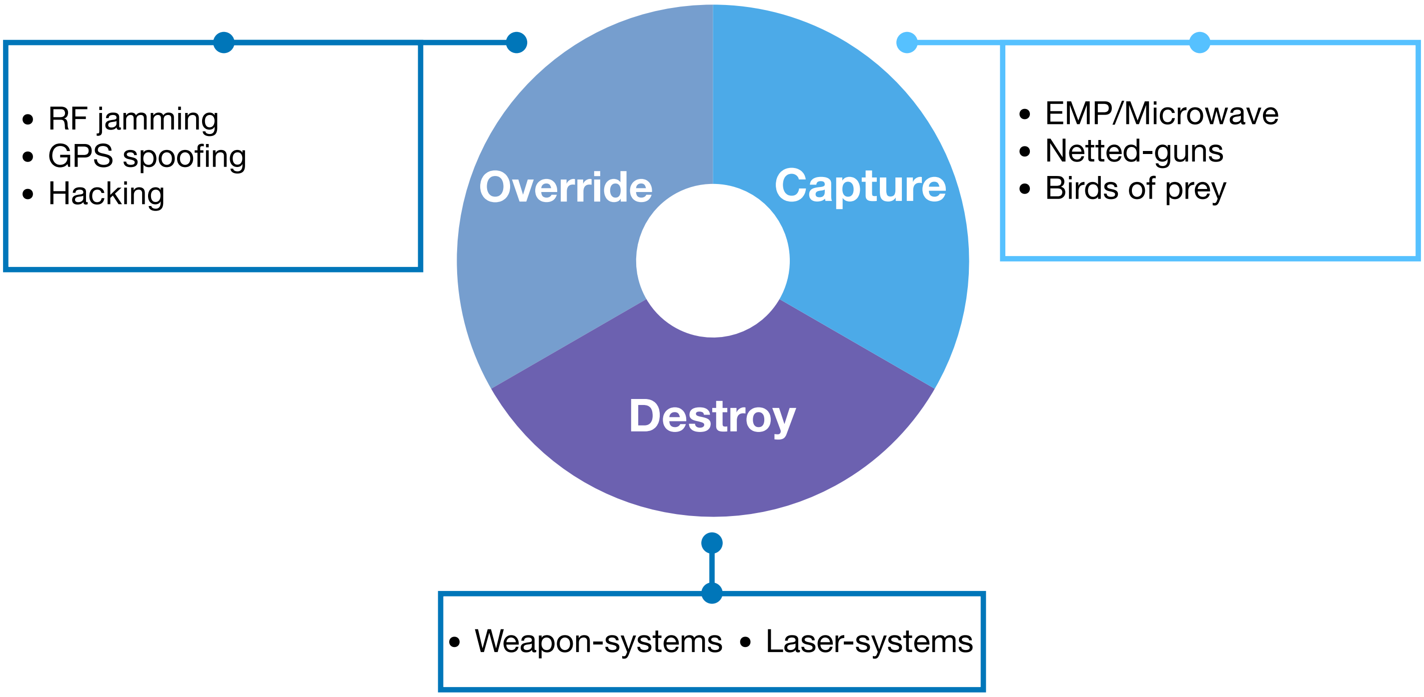
Imaging & Reflection

- **Holographic radars**
- **High-definition cameras**
- **Thermal imaging**

In the first category, radio frequency detection involves analysing the frequency of the radio waves used to communicate between the operator of the drone and the drone itself. Most drones will utilise frequencies in the range of 2.4 to 5.2 GHz for both control and video, which if analysed properly, will allow the accurate detection of a drone. Using multiple types of this detector, the drone position and sometimes even the operator, can be triangulated. However, FPV drones typically use between 800-900 MHz transmitters with advanced self-healing networks and frequency hopping technology, which can make it difficult to track or jam the signal of such a drone. Acoustic detection meanwhile is a highly accurate detection system, with correct identification rates as high as 97%, however in a noisy environment where sound sources such as aircraft are much louder, they become ineffective [35].

Imaging and reflection techniques can provide a means of accurate detection of drones. Holographic radar is an advanced form of radar which can scan with very low latency and detect small objects, making it a useful technique for identifying drones [36]. Camera systems, both thermal imaging and high-definition optical sensors can also provide accurate identification of drones, however usually in a perfect environment of a dark drone against a monochromatic sky. As technology advances, and AI image processing is applied to these technologies, they should become increasingly robust and accurate [37]. If a drone has been successfully detected, countermeasures could be employed to mitigate the danger of the drone. Countermeasures can be divided into three categories; destructive techniques, capture techniques, and finally overriding techniques, see figure 7 below. All of these countermeasures generally rely on exploiting the vulnerabilities of the technology or operation of a given drone. With the override type, both RF jamming and GPS spoofing rely on both the drone using these technologies, and the semi-autonomous behaviour of consumer drones. That is, most consumer drones are programmed to land if they lose signal GPS or radio signals, however, some drones (such as FPV drones) wont use these technologies and have no such programmed behaviour. Meanwhile, RF jammers are devices which emit a concentrated beam of radio frequency energy to confuse the drone. They require the user to accurately track the drone with the device until it lands, and are generally effective within 100 m [37]. This may work with slow or static consumer drones, but is much more challenging on a fast moving, and highly agile FPV drone. Hacking is also a possibility, for certain drones [37], but relies on the drone using sophisticated software, something which FPV drones usually lack, using basic programming only, and few on-chip interfaces.

Figure 7 **Three types of countermeasures**



Capture techniques again require the drone to be accurately tracked, and in most cases also require close proximity. Microwave emitters can fire a targeted electromagnetic pulse at the drone, which could disrupt or damage the electronics of a drone. Currently, handheld options have low power and range, but high power turrets and command centres could be significantly more effective [37]. Birds of prey have also been utilised to capture drones in Amsterdam to counter drug smuggling, however they require extensive training and are limited towards slower drones [38].

Finally, the destroy method whilst potentially highly effective, also comes with a set of risks and dangers. Weapon-systems for example, such as the Phalanx CIWS, have been used by the US navy as a ‘last resort’ measure against close proximity missiles and aircraft [39]. It can accurately track and destroy missiles by firing bullets at an extraordinarily high rate. Such a system could potentially be adapted for use against drones; however the accuracy would need to be significantly increased, it would not work against swarms of drones, and it would be highly unlikely such an autonomous live-ammunition weapon-system would ever be permitted in a civilian context. Lasers are a promising new technology, which can engage over much longer range and deliver high levels of directed energy towards a drone. With continued improvements to tracking technology, and improvements to the power of laser systems, such a tool could be used in the future to quickly and safely dispatch drones. However, most of this technology is still in development phase with the military and the power of the lasers is too low for quick effect against small fast drones [37]. Figure 8 illustrates how effective these various detection and countermeasure systems might be against a typical drone from each of the three classes considered (where green = effective, red = ineffective, and orange = unclear). The FPV class is difficult to define due to the extensive configurability; an FPV drone could be designed to avoid these detection systems and countermeasure systems if the operator or designer wished to.

Figure 8

Effectiveness of detection and countermeasures against civilian drones

		Consumer drone	Commercial drone	FPV drone
Detection systems	RF detection	Known codes + frequencies	May not use RF	May not use RF
	Acoustic detection	Local noise can prevent detection	Local noise can prevent detection	Local noise can prevent detection
	Holographic radar	Accurate tracking + known models	Often larger, easier detection	Speed + design may confuse system
	HD cameras	Slow moving, known shapes	Large, slow moving	Fast, low flying, different designs
	Thermal imaging	Known thermal signatures	Can be masked with design/ducts	Speed cools drone, design can mask
Countermeasure systems	RF jamming	Known codes + frequencies	Might not use RF (high autonomy)	High fidelity RF + can use 3G/4G
	GPS spoofing	Some drones without GPS	High autonomy, high GPS usage	Little GPS/compass usage
	Hacking	Familiar software	Can be custom software	Too simple/ unsophisticated
	Microwave	Shielding/plastic less effective	Shielding/plastic less effective	Too fast (tracking required)
	Netted guns	Slow, effective close range	Large, effective close range	Too fast (low range)
	Birds of prey	Effective if trained	Can be too large for a bird	Too fast + many different designs
	Weapon-systems	Too small (or dangerous)	Large; can work in non-civilian areas	Too small (or dangerous)
	Laser-guided	Technology not fully developed	Technology not fully developed	Technology not fully developed

Considering the commercial airliner example in section 2, we can examine the above systems for an FPV drone with their expected effectiveness.

- **RF detection**: Many FPV drones utilise high fidelity transmitters and receivers (operating in the 800-900 MHz range), with advanced self-healing networks, making detection more difficult [40].
- **Acoustic**: will likely be highly ineffective in an airport due to the excess ambient noise.
- **Holographic radar**: Heathrow and other global airports have holographic radar systems, however they may not be able to discern an FPV drone from a bird (due to the fast and sporadic low altitude flight paths).
- **Camera systems**: Could become highly effective with increasing applications of AI in computer vision, however against backdrops of trees and grass, these techniques may be ineffective.
- **RF jamming/hand-held microwave/netted guns**: As these techniques all involve a human physically tracking the drone, it's likely to be too difficult to maintain a solid lock on these very fast and agile drones. They are only effective if sustained.

This paints a worrying picture for the safety of an airport against an attack of this nature, and to the best of this authors knowledge, there are very few solutions that would work now against this threat. The continuing research in laser technology is likely to be a good future solution, and probably the only acceptable destructive method in a civilian context. Currently the consensus of security experts is there is no 'one perfect' solution, and the best approach with these technologies is to use many of them as possible for maximum protection [41].

Section 4: Doomsday scenario

In this next section, we consider the hypothetical question; just how bad, with some imaginative thinking and near-future technology, could the threat of a weaponised drone really be? For this, we consider a scenario where micro-sized swarms of drones, with sophisticated on-board computers, are used against the civilian population of a metropolitan area.

There are many micro-sized drones available today, such as the military Black Hornet Nano (weighing just 18g), which is capable of advanced vision processing from multiple on-board cameras [42]. In the near future, we can expect these drones to become even smaller, and have even more functionality. Considering the current trends in the development of openAI, and wider public access of these toolkits, it could be possible that a computer-vision based program is installed in these very small drones, along with a deadly payload (such as the nerve agents previously analysed, or a micro-explosive). With such software and hardware, the drone would be able to accurately process images in real-time, using the on-board computer, to intelligently navigate to its target; seeking out whatever the operator has programmed it to seek. This could for example be to visually identify humans, and then engage or harm them, or perhaps to target certain races, ages, or genders of a population, selectively attacking them. This kind of selectivity would allow an operator with malicious or political motivations to target with prejudice.

Such a drone would be nearly impossible to detect or stop, but the real formidableness of this system would come from applying it at scale; with a swarm of these drones perhaps 10,000 or more. Considering the micro-size, the cost of these drones is likely to be very low within the next 10-15 years. Even as our countermeasures become more advanced, they will be significantly difficult to target as they could be fully autonomous and pre-programmed; electronically isolated from the outside world with sufficient shielding and protection. The estimated loss of lives of such an attack would be unimaginable.

Conclusion

In this essay we have explored the various different types of drones that are available today, and the different risks that these devices can present to national security. Investigating these risks, a number of real-life instances were elaborated, showing in many cases the culprit is often not identified. It has been shown how current security systems are not capable of dealing with these new risks from drones, and to this extent, two high-risk scenarios that are possible today were examined. Having identified these high-risk scenarios, the current tools and systems for countering drones were analysed with respect to the different types of modern highly-accessible drones. It was shown that these countermeasure systems are largely ineffective against FPV drones, and have varying levels of effectiveness against consumer and commercial type drones. Of course, as stated, the level of effectiveness depends heavily on the drone in question and the technology it utilises. Finally, a doomsday scenario was imagined; using current or near-future technology, a devastating and massive attack on people could be selectively carried out with effectively few options to prevent it. It is the authors recommendation that technology companies and government consider more urgently the threat of these types of drones, and develop new technologies to help better counter them in these high-risk situations.

[1] - Timothy Amukele, Using drones to deliver blood products in Rwanda, Lancet, Vol. 10, 4, Pg. 463-464, April 2022, 10.1016/S2214-109X(22)00095-X
[2] - Lilium.com
[3] - P. Planing, and Y. Pinar, Acceptance of air taxis - A field study during the first flight of an air taxi in a European city, Center for Open Science, Dec. 2019, 10.31219/osf.io/rqgpc
[4] - Certification Specifications for Large Aeroplanes, EASA CS-25, European Aviation Safety Agency, 2007
[5] - “Ukraine Is Fielding A ‘Heinz 57’ Fleet Of Heavy Drone Bombers Against Russian Forces”, - David Hambling, Forbes, Dec. 2022.
[6] - “The mystery of the Gatwick drone”, - Samira Shackle, The guardian, Dec. 2020.
[7] - Price of DJI Mini 3 (varying between £349 and £569 for various models), April 2023, https://store.dji.com/uk/
[8] - "Drones Are Weapons of Choice in Fighting Qaeda”, - Christopher Drew, The New York Times, Mar. 2009.
[9] - “China drone maker DJI: Alone atop the unmanned skies”, - Joshua Bateman, CNBC Disruptor 50, Sept. 2017

[10] - The Drone and Model Aircraft Code, Open A1 and A3 categories, The UK Civil Aviation Authority, 2019

[11] - "How To Get Started With FPV Drone – The Ultimate Beginner's Guide", - Oscar Liang, personal blog, Feb. 2023

[12] - "Ukrainian Commandos Decimate Russian Mechanized Force Using Racing Hobby Drones", - Sebastien Roblin, Forbes, Dec. 2022.

[13] - "Ukrainian Drone Drops Bomb Through Open Hatch To Score First Kill On Russia's Oldest Tank" - David Hambling, Forbes, July 2022.

[14] - "In a Ukraine Workshop, the Quest to Build the Perfect Grenade", - Thomas Gibbons-Neff and Natalia Yerma, The New York Times, Jan. 2023.

[15] - "A Drone Tried to Disrupt the Power Grid. It Won't Be the Last", - Brian Barrett, Wired.com, Nov. 2021.

[16] - "Drug smuggling: Underwater drones seized by Spanish police", - Leo Sands, BBC News, July 2022.

[17] - "'Like a flying ant': An operative describes how Mexico's cartels use drones to attack enemies and smuggle drugs", - Luis Chaparro, The Business Insider, June 2021.

[18] - "'Drones causing mass trauma among civilians,' major study finds", - Chris Woods, The Bureau of Investigative Journalism, Sept. 2012.

[19] - "How Wi-Fi spy drones snooped on financial firm", - Thomas Claburn, The Register, Oct. 2022

[20] - "Governments Are Using Drones to Spy on Americans. Here's How People Are Fighting Back", - Patrick Carroll, Fee Stories/FEE.org, Nov. 2022.

[21] - M. Shahrooz, A. Talaeizadeh, A. Alasty, "Agricultural Spraying Drones: Advantages and Disadvantages", 2020 Virtual Symposium in Plant Omics Sciences, IEEE Xplore, Sept. 2021, 10.1109/OMICAS52284.2020.9535527

[22] - Skykrafts Aerospace, Kisan Drone (Beta), https://www.skykrafts.com/product/kisan-drone/

[23] - F. R. Sidell, "Medical Aspects of Chemical and Biological Warfare", 1997 p. 142.

[24] - "Kim Jong-un's half-brother dies after 'attack' at airport in Malaysia", - Justin McCurry and Emma Graham-Harrison, The Guardian, Feb. 2017.

[25] - "Salisbury poisoning: Police 'identify Novichok suspects'", - BBC News, July 2018

[26] - "Toroidal Propellers", - MIT Lincoln Laboratory, U.S. PATENT #10,836,466, MIT, 2022.

[27] - "Music festivals: a high-risk business", FT Film, P. Gioumpasis, Sept. 2021.

[28] - D. Bradley, "VX Nerve Agent in North Korean's Murder: How Does It Work?", Chemistry world, Scientific American, Feb. 2017

[29] - "A Beginners Guide to FPV Drones", Rotor Riot, Orlando, FL 32822, rotorriot.com

[30] - European Aviation Safety Agency: Drone collision task force, European Aviation Safety Agency (2016)

[31] - Y. Song et al., "Investigation of UAS ingestion into high-bypass engines, part 1. Bird vs. Drone", The 58th AIAA/ASCE/AHS/ASC structures, structural dynamics, and materials conference, American Institute of Aeronautics and Astronautics (2017).

[32] - H. Chen et al., "An experimental study on thermal runaway characteristics of lithium-ion batteries with high specific energy and prediction of heat release rate", Journal of Power Sources, Vol. 472, Oct. 2020.

[33] - "Droning on about geofencing: A deep dive into the world of drone restrictions and boundaries", - XDynamics Evolve 2 blog, Jan. 2023, https://www.xdynamics.com/blog/drone-geofencing-faq

[34] - Anti-Drone 2023-2033 report, Oliver Davison, Visiongain Reports Ltd., Mar. 2023

[35] - H. Lv et al., "Drone Presence Detection by the Drone's RF Communication", J. Phys., Conf. Ser. 1738 012044, 2021.

[36] - S. Harman et al., "The Need For Simultaneous Tracking And Recognition In Drone Surveillance Radar", 2021 21st International Radar Symposium (IRS), IEEE Xplore, 2021.

[37] - J.P. Yaacoub, "Security analysis of drones systems: Attacks, limitations, and recommendations", Journal of Internet of Things, Vol. 11, Sep. 2020, 100218.

[38] - "Dutch Firm Trains Eagles to Take Down High-Tech Prey: Drones", - Stephen Castle, The New York Times, May 2016.

[39] - "20 mm Phalanx Close-in Weapon System (CIWS)", - Tony DiGiulian, NavWeaps.com, Mar. 2018.

[40] - TBS Crossfire TX - Long range R/C transmitter, product by TBS Blacksheep, https://www.team-blacksheep.com/products/prod:crossfire_tx, Mar. 2023.

[41] - "10 Counter-Drone Technologies To Detect And Stop Drones Today", - Robin Radar Systems, 2023 sales promotion report (specialist anti-drone systems).

[42] - Black Hornet PRS, Teledyne Systems, product systems page: https://www.flir.co.uk/products/black-hornet-prs/?vertical=uas-norway&segment=uis, accessed Mar. 2023.