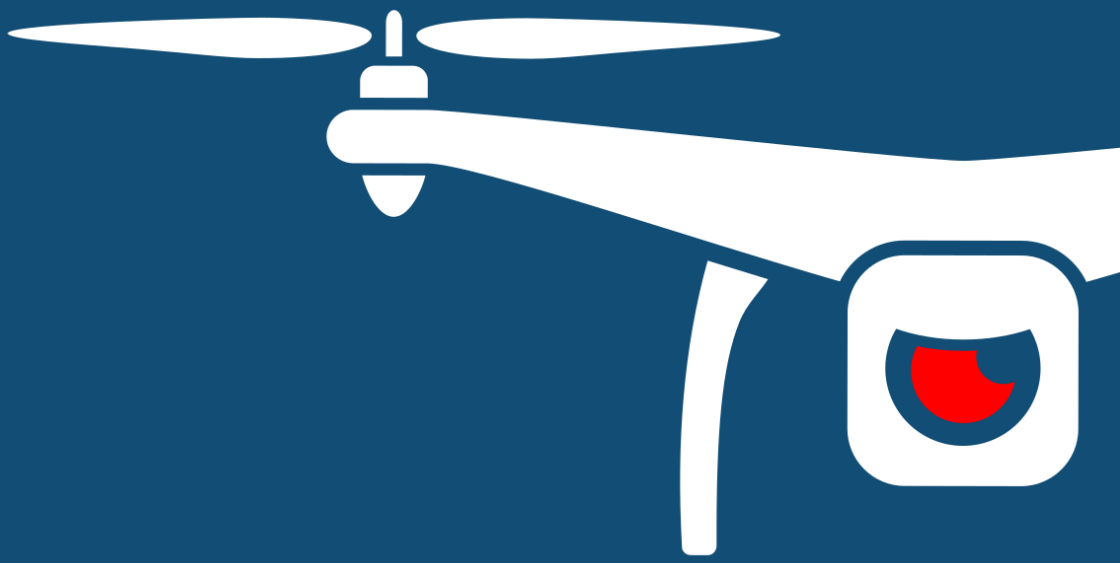
DRONE SEC
A Privasec COMPANY

NOTIFY ISSUE #25

WEEKLY THREAT INTELLIGENCE

03 June 2020 | v1.0 RELEASE



UAS HACKING, HARDENING AND DEFENCE

UAS PENETRATION TESTING
COUNTER-UAS CONSULTING
FORENSICS & INCIDENT RESPONSE
AERIAL THREAT SIMULATIONS
DRONE SECURITY MANAGEMENT PROGRAMS

DOCUMENT **CONTROL**

PREPARATION

DroneSec (dronesec.com)

Threat Intelligence Team

Email: info@dronesec.com

Phone: 1800 996 001 | + 614 7854 3434 (Urgent)

EXECUTIVE SUMMARY

Wherever you are in the world, the DroneSec team hopes you are safe, and your respective families are doing well.

As with every large-scale event, our signal-to-noise ratio needs to re-learn what is normal vs "event driven". For example, during COVID-19 our artefacts have had to reflect that some 'incidents' are simply involving drones rather than the drone being the subject. As with the recent George Floyd protests, we have a number of drone-related footage and use popping up, but not directly related. One very interesting scenario is Customs and Border Protection using a predator drone to provide surveillance and monitoring over the city of Minneapolis, USA – in fact it's the only Law Enforcement use of drones during the protests that we've witnessed so far. There is now an investigation into the legitimacy of its use and lawfulness.

In this issue, Teal Drones release details of their DoD-compliant secure, rugged and American-made systems aimed at law enforcement and military use. Cloncurry UAS Flight Test Range opens up in Australia and the Indian city of Sircilla links their drone cameras to a live-feed operations centre – not to mention the addition of one drone pilot per law enforcement vehicle.

Some interesting movements in the Counter-UAV space, with Blighter Systems looking to position in Australia, DeDrone partnering with BlackBerry (traditionally cyber-security and intelligence) and DroneALERT launching their newly-updated rapid drone reporting and intelligence system.

While it may not be sitting in a physical box, the most recent DroneALERT announcement got the DroneSec team pretty excited. It's currently the only community-reporting solution that fills evidence gaps in a drone incident. Public reports are cross-referenced with internal metrics and delivered straight to Law Enforcement for triage. A number of potential use cases where this will be useful and paves the way for innovation in the field whilst reducing the risk of increased restrictions on legitimate fliers. There is a genuine need for agnostic, independent organisations dedicated to drone security within our industry sector.

I'll keep this one short as there's a fair bit of quality statistics, trends and patterns in our monthly roll-up to get through. As always, if you have comments or feedback, or want to join in the discussion in our slack group, please don't hesitate to contact us.

- *Mike Monnik, DroneSec CTO*

TABLE OF **CONTENTS**

1. Threat Intelligence ---- 5
1.1. Introduction ---- 5
1.2. Monthly Roll-up ---- 6
1.3. Featured Advisories ---- 14
1.4. News and Events (P3) ---- 18
1.5. Whitepapers, Publications & Regulations (P3) ---- 19
1.6. Counter-Drone Systems (P4) ---- 19
1.7. Informational (P4) ---- 20
1.8. Social (P4) ---- 21
1.9. Drone Technology (P5) ---- 22
APPENDIX A: Threat Notification Matrix ---- 23
A.1. Objectives ---- 23
APPENDIX B: Sources & Limitations ---- 27
B.1. Intelligence Sources ---- 27
B.2. Limitations ---- 28

1. THREAT INTELLIGENCE

1.1. INTRODUCTION

Threat Intelligence to the DroneSec team means cutting-edge information, news, resources and threats delivered in a succinct and actionable way. Notify is just that – key information that can be used to prepare, prevent and identify threats and challenges which seek to take advantage of the drone industry. Our aim is to allow organisations to make more informed decisions, respond effectively and get a birds-eye view of our core focus: Drones, Counter-Drone and Universal Traffic Management (UTM) Systems – also referred to as **DCU**.

When it comes to proactively seeking out the best solutions, developing response capabilities or building resilience into your drone operations, relevant information is king. We're dedicated to ensuring you stay up to date through Notify, while getting the specific details around techniques, vulnerabilities, targets and malicious actors. Furthermore, we've made all Notify information both scalable and easily categorised, providing a mechanism for easy search but also extraction of statistics and use cases for stakeholders who need pre-mitigation insights and strategies.

For technical operators, we've included the ability to be able to prioritise relevance over noise and communicate with each other to exchange ideas and collaborate on threats. This exchange happens on a number of levels, from our slack channel, to sharing DroneSec case-studies within the platform and hearing from our partners (individuals, technology vendors, law enforcement and regulatory bodies) who supply valuable information to Notify.

Weekly reports are just that – the lifespan only covers one week of intelligence and where this might extend is when we detected or were alerted to it later on. You can rely on this information not being too old or outdated; but you're always able to browse the archives and library for older artefacts. Anything breaking news, we send off immediately to our Notify subscribers – outside of this, the report covers the rest on a weekly basis.

So how does it all work? To view our methodology, sources and scoring matrix, head down to the appendices to get a feel for it all. Otherwise, information we deem as being 'key' is featured with insights and analysis supplied for reader's benefit. The rest of the information we pick up that can be categorised as security-based intelligence for DCU is placed thereafter. Our categorisation and tagging system mean that on a monthly basis, you'll get an overview of the statistics we've seen – updated in real-time, week-on-week for pattern recognition analysis.

Kicking it all off, we're delivering our first few rounds in PDF format. In the next few weeks, we'll continue to roll out platform access to ensure we can sustainably support our current client needs with relevant, actionable information within the context of DCU.

Something we missed? Keen to become a supplier? Want to join the Notify platform? Shoot us a message at info@dronesec.com. Otherwise, feel free to hop into the slack channel and introduce yourself: DroneSec Slack Channel. If you missed the previous issue, please email us.

1.2. MONTHLY ROLL-UP

As we enter the month of June, Notify features an aggregated summary of drone incidents, types and affected sectors in the past months of 2020 and collated numerical data on drone incidents for the year. Extended analytics with full database-searchable functionality is only offered to our Plus and Premium members, with improvements currently taking place on the platform.

Below you'll find some handy statistics to measure correlation, location and systems involved over data we've collected since January 2020. Anything we've missed? Anything you'd like to see? Drop us a note at info@dronesec.com to get in touch with the team.

In 2020 thus far, eight hundred and forty-five artefacts were recorded which roughly equates to 5.56 drone security incidents/events **per day.**

Month	Number of Artefacts	Global number of incidents per day	Month-on-month increase
January	135	4.3	N/A
February	139	4.8	4 (2.88%)
March	179	5.8	40 (22.34%)
April	192	6.4	13 (6.77%)
May	200	6.5	8 (4.00%)
Total (2020)	**845**	**5.56**	N/A

The number of events logged has increased significantly in the past three months mainly due to the widespread use of drones to monitor and restriction movement of citizens globally in an attempt to curb the spread of COVID-19. The use of drones has also complemented the efforts of local law enforcement agencies with its electro-optic and thermal cameras for surveying, then apprehending (hiding) offenders with servicemen on the ground. Drones have proved effective in this aspect and more law enforcement agencies are starting to see the benefit of it.

Similarly, some organisations and local retail owners are taking this opportunity to use drones (albeit legally or not) creatively to continue their sales or overcome the lockdown restrictions. We see collaboration between medical, construction and agricultural firms with organisations offering drone services for the delivery of supplies or conducting of work offsite. Local retailers are using commercial drones to deliver their products to better reach their customers who are stuck at home.

Drones have complemented traditional processes and proved to be more effective.

DroneSec monthly rollup tracks incidents, events and these categories/tags allows readers to visualise them on a month to month basis. The statistics below are for the month of January to May 2020: Notify release #4 – #24.

We see a 45% increase in Featured Articles in the month of May 2020. Ten of the incidents were related to illegal deliveries of contraband into prisons via drones; these incursions accounted for 48 per cent of all the Featured Articles in May. Six of the Feature Articles (29%) were incidents of drones flown in close-proximity or had an illegal infringement into aerodromes or airspace of manned aircrafts. While drones are beneficial towards enforcement agencies and local retail owners, organised crime syndicates have also found themselves a new tool to conduct their nefarious activities.

Category	Number of Artefacts (Jan - May 2020)	Number of Artefacts (Jan - Apr 2020)
Featured	46	25
Cyber and Information Security	18	13
News and Events	217	181
Whitepapers and Publications	133	109
Counter-Drone Systems	71	58
UTM Systems	39	30
Drone Technology	89	67

Organised crime syndicates have also found themselves a new tool – drones.

DroneSec has collected a number of statistics for the year 2020 and we saw a staggering number of contraband deliveries made to prison via the use of drones. Out of these cases, only 56% of the drones were seized by the law enforcement bodies. Some prisons were well equipped with Standard Operating Procedures (SOP) on handling drone incursions and were able seize the opportunity when a drone was spotted, whereas others were not successful in their attempts. In one of the cases that DroneSec recorded, the drone was taken down with the help of residents who reported the suspicious activity. Of the 56% of drones seized, 57% of the operators were apprehended while the remaining 43% were either not located or managed to escape. If a greater number of operators are located when a drone is seized, this could imply they are attempting to retrieve or locate their drone, putting themselves at risk of being apprehended in an attempt to remove evidence. Further analysis is required in order to properly ascertain this however, given that sometimes apprehensions take place without seizure of the drone system.

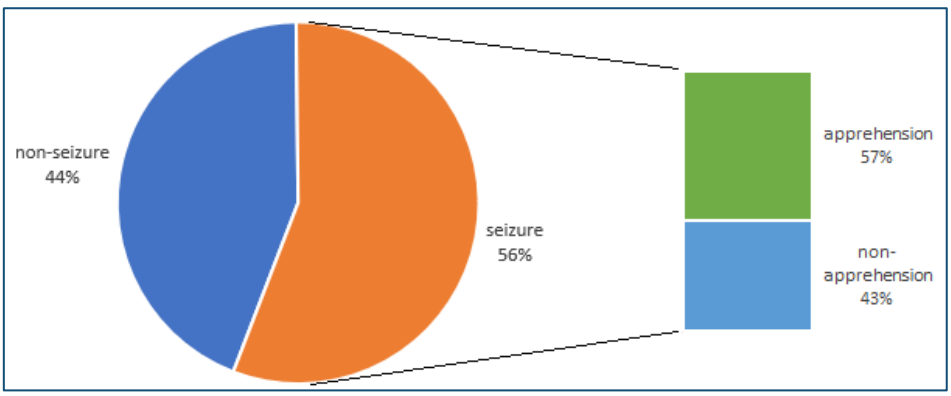


Figure 1: Percentage of contraband deliveries to prisons where the drone was seized and/or operator apprehended

Other than drone-prison deliveries, DroneSec saw a number of airspace infringements by drones as well, some led to collision with manned aircrafts, some caused a shutdown in the aerodrome for hours and others caused delays for medical aviation vehicles. Unlike prison infringements, it is much harder to sight a drone within the airspace size over an airport, let alone seize it without affecting the legitimate aircraft. Of the cases that were recorded, only 35% of the drones were seized – however, 100% of seizure cases resulted in their operator(s) being caught in the act (note: not all of these intrusions were nefarious in nature).

Drones are small, fast and more versatile in escaping from the detection of law enforcement agencies. Nefarious operators will use this to their advantage and flout drone laws to conduct their illegal activities.

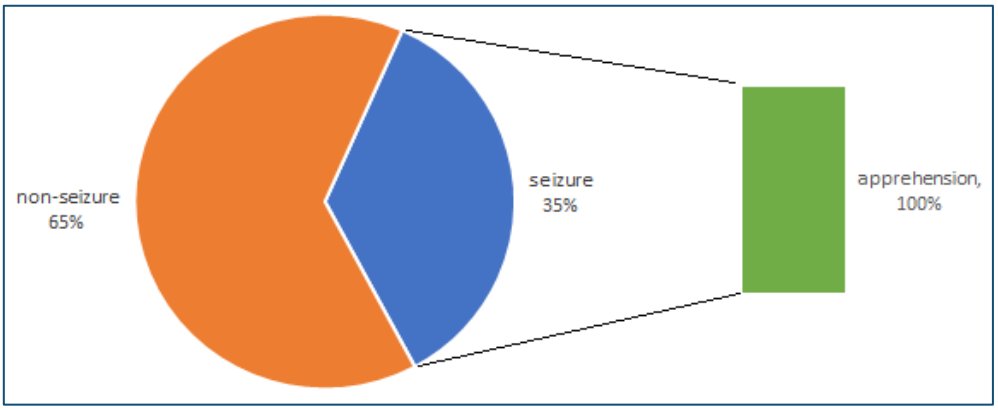


Figure 2: Percentage of illegal infringement into airspace where the drones was seized and/or operator apprehended

On the larger scale of things, drones are beneficial and serve to improve the quality of life and standard of work for families and organisations who are badly affected by the pandemic. Government and regulators around the world have been opening themselves up for more drone trials and some extending to Beyond Visual Line of Sight (BVLOS) operations where drones are allowed to fly across tens of kilometres out of visible range from its operator. However, authorities also do know the risks that are inherent with drones and are actively managing and working with the community to combat against operators who intentionally use drones for illegal purposes.

-

Drones are versatile and more likely to escape visual detection. Criminals will use this to their advantage.

Continuing on, we've gathered some of the key metrics around specific events and the drones involved. This can help assess historical data and determine if patterns exist amongst similar events. Since January 2020, we have collated several incidents where drones have flouted law and an increase in the number of cases involving illegal infringements and contraband deliveries.

May 2020 saw a large increase (10+ cases) in number of contraband drone deliveries. DroneSec advocates for protected and restricted facilities to adopt procedures relating to drone incidents; however, much of this industry participation relies on the governmental judicial and executive arms prioritising the importance of having counter drone measures in place in order to better prevent, or reduce, the occurrences of such events. Procurement of counter drone systems may be required to

undergo a lengthy process due to the extensive staff work within the government bureaucracy. In addition, agencies must also take time to carry out tabletop simulations to better determine the exact communication flow and processes required for drone incidents. Critical infrastructure facilities such as prisons and territorial borders with frequent incursions should prioritise the development of counter-drone measures to guard against rogue drones.

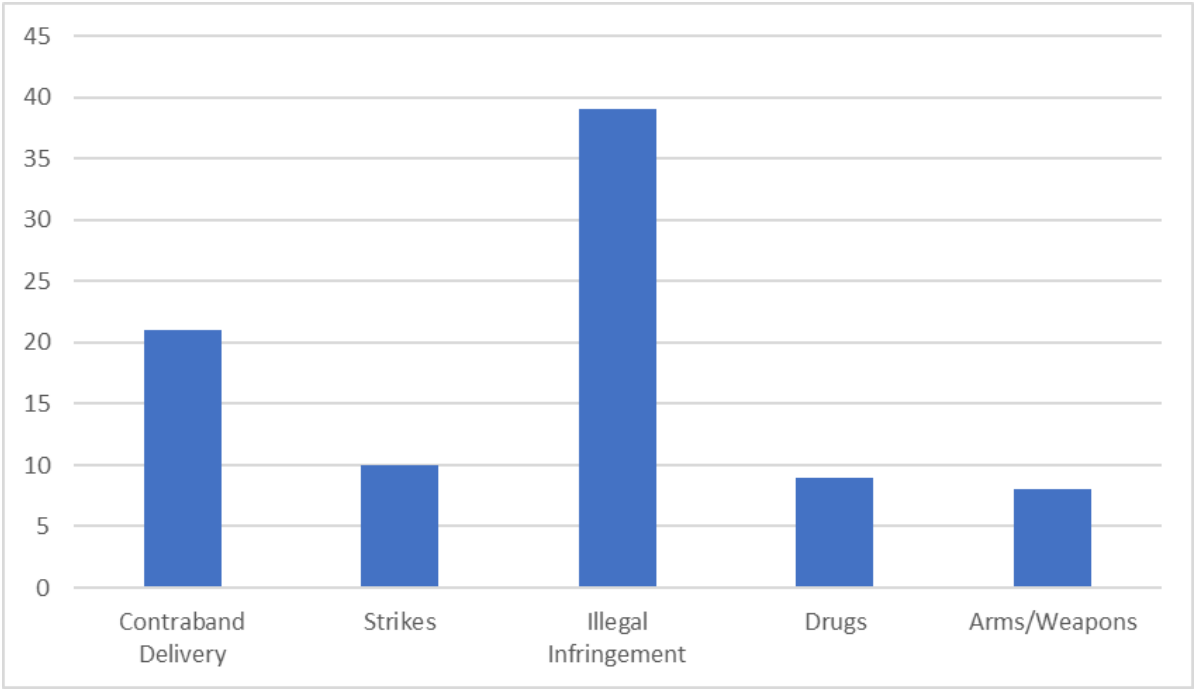


Figure 3: Number of Drones Utilised by Category of Activities (Since January 2020)

-

In May 2020, we saw more drone infringements happening at prisons and residential neighbourhoods as compared to April 2020. There were multiple artefacts on attempted contraband deliveries via drone-drops within prisons and invasion of privacy nearby residential homes.

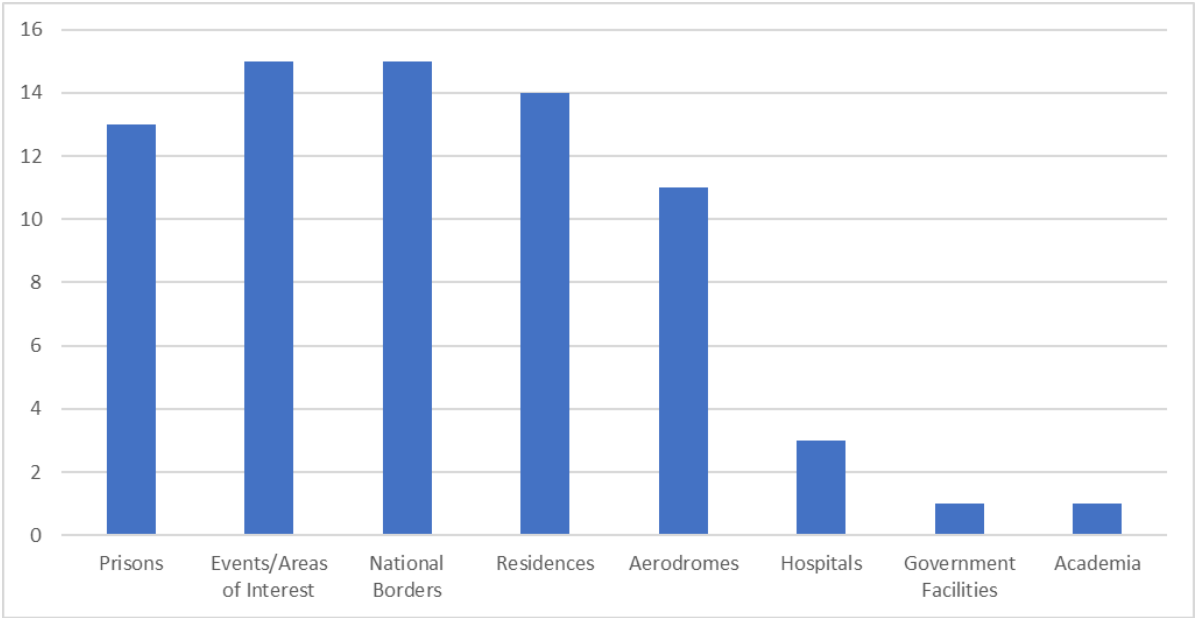


Figure 4: Number of Drone Incidents by Location of Occurrence (since January 2020)

Drones are still positioned as a relatively safe method of conducting illegal activities, due to the physical separation of the operator from their device and the lack of law enforcement strategies. Traditional means of securing perimeters with barbed wires and erected fences no longer provide adequate security and air defences against small unmanned drones. However, on the flip side, many counter-drone systems do not provide a 'silver-bullet' cost effective solution against easily available and cheap quadcopters. The current economic ratio of counter drone systems which cost between $10,000 - $1,000,000 against a $500 - $10,000 commercially available drone is still very much to the malicious operator's advantage.

DroneSec often advises perimiter protection and asset security management teams in following a customised plan if a counter-drone or detection system is not readily available:

Traditional means of securing perimeters with barbed wires and erected fences no longer provide adequate security and defences against small unmanned drones.

1) Have a drone security management plan in place to deal with small unmanned systems. A Standard Operating Procedure (SOP) should aid govern the process, people and methodology in handling a drone, collecting evidence and responding to potential operators in a predetermined radius around the perimiter grounds.

2) Undertake mock simulations as Table-Top exercises in reacting to both in-air and downed drones to hone responses, improve communication flow between agencies and practice on the logging and monitoring of repeated drone drop off cases.

3) Monitor, and recognise patterns and trends (such as origin of flight, time of day) to help provide the modus operandi of rogue groups and potential identification and arrest of rogue operators.

4) Have a drone forensic extraction and incident response kit readily available to aid in the preservation of evidence and identification of offenders.

-

As DroneSec Notify records the number of drone incidents and events happening around the world, we see that majority of drone users come from the USA, India and the UK. Majority of the artefacts from these countries have seen drones implemented country-wide into (1) law enforcement agencies – to help police enforce security and arrest runaway criminals, (2) government agencies and organisations – to perform checks on vast areas of land, infrastructure or medical deliveries, and also (3) commercial and hobbyist lifestyles such drone lighting visual aerial displays, technological research and advancement, or deliveries of food and/or essentials.

Other countries like Africa, Australia, Japan, Canada are also rapidly advancing in their use cases of drones. We have seen articles on collaboration of drones with existing industries in the maritime, energy, and agricultural sectors. Countries who are early adopters of drones have had an increase in discussions around drone regulations during COVID-19. Adhering to these regulations help the drone community exist cohesively with the public and other manned/unmanned aviation sectors. Unsafe and

unwarranted acts will only serve to impose more stringent rules to the drone community and further tarnish the utility of drones within the public's perception.

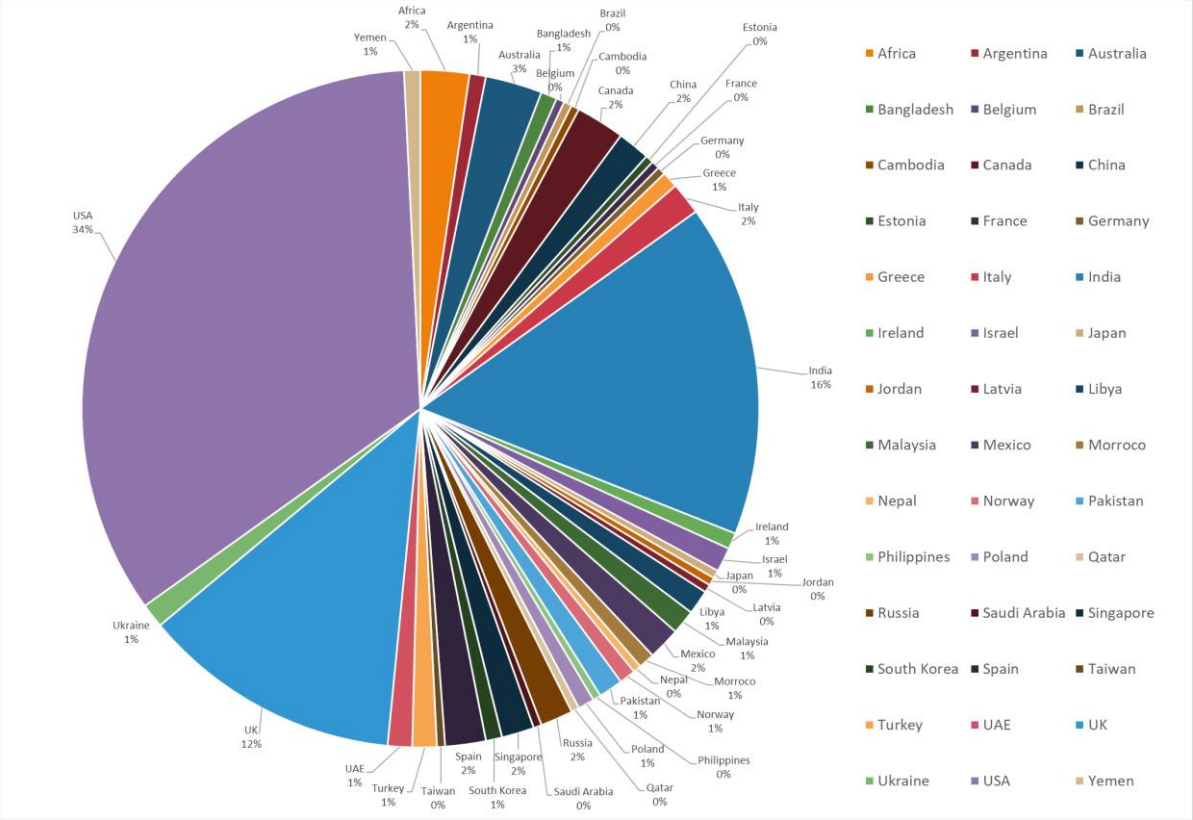


Figure 5: Percentage of Drone Artefacts by Country of Occurrence (Since January 2020)

-

DroneSec record the make and model of each drone from the artefacts recorded so that law enforcement and counter drone industries can better prepare themselves with appropriate measures against commonly used drones. It is not surprising to see a majority of drones used were from the Chinese brand, DJI.

DJI have been a main and primary market leader in small unmanned drones, leading in technological advancement in the utility of drones from hobbyist to commerical to customised drones specially suited to certain needs. Progress and breakthrough of drones within DJI have been fast in the recent years which have led to their success and profileration globally. In addition, DJI manage to continually develop drones that are able to fall within global guidelines and regulations (size, weight, remote identification).

Unsafe and unwarranted acts will only serve to impose more stringent rules to the drone community and further tarnish the utility of drones within the public's perception.

Interestingly, while the DJI drones are popular amongst security agencies, law enforcement across the globe have differing preferences on drone acquisition. India prefers the DJI Phantom models and the Indian made Netra and Multiplex drones. The UK and the USA prefer the DJI Mavic and Matrice models, albeit the various restrictions regarding overseas made drones raised in the USA. In addition,

a review of exisitng law enforcement agencies have shown that most who possess multiple drones tend to have a DJI drone to augment their existing fleet.

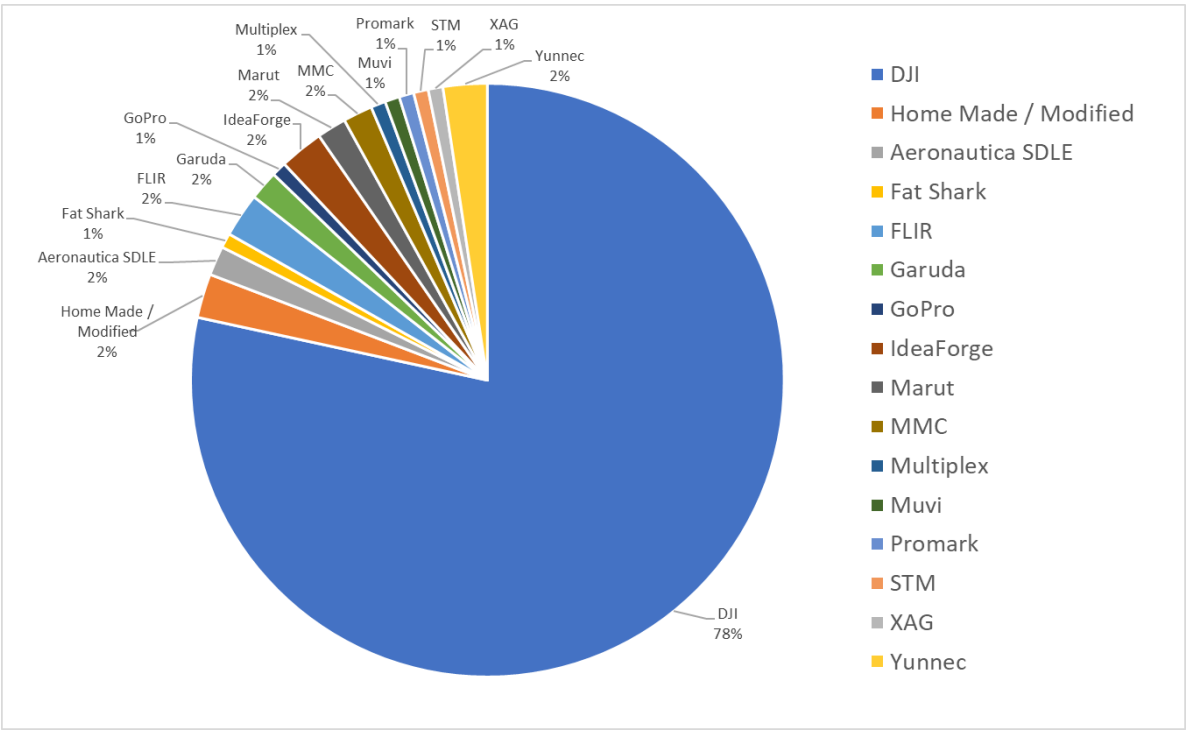


Figure 6: Percentage of Brands of Drones Utilised (Since January 2020) from our recorded artefacts. <1% is displayed as 1%.

Within DJI drones, the most popular model logged is the Mavic series. The DJI Mavic is versatile in many kinds of surveillance operations as it is light weight, fast and portable. It has gained popularity amongst hobbyists, law enforcement, government and security agencies due to its capability in carrying multiple sensor payload (thermal and electro-optic), fast speeds of up to 72km per hour and its small and portable cross-section footprint.

Following that, the DJI Matrice has the capability to carry high payloads which allows a wide variety of attachments for varied uses. Government organisation and agricultural sectors usually champion the use of the DJI Matrice due to its capability to perform multiple tasks which help offload the need for a man on the ground performing labourous work under unfavourable weather. With the recent release of the Matrice 300, and already artefacts emerging targeting that system, the next few months of analysis will continue to compare this.

India law enforcement agencies predominantly use DJI Phantom drones and the Indian made Netra and Multiplex drones; whereas the UK and the USA law enforcement bodies predominantly owns the DJI Mavic and Matrice models.

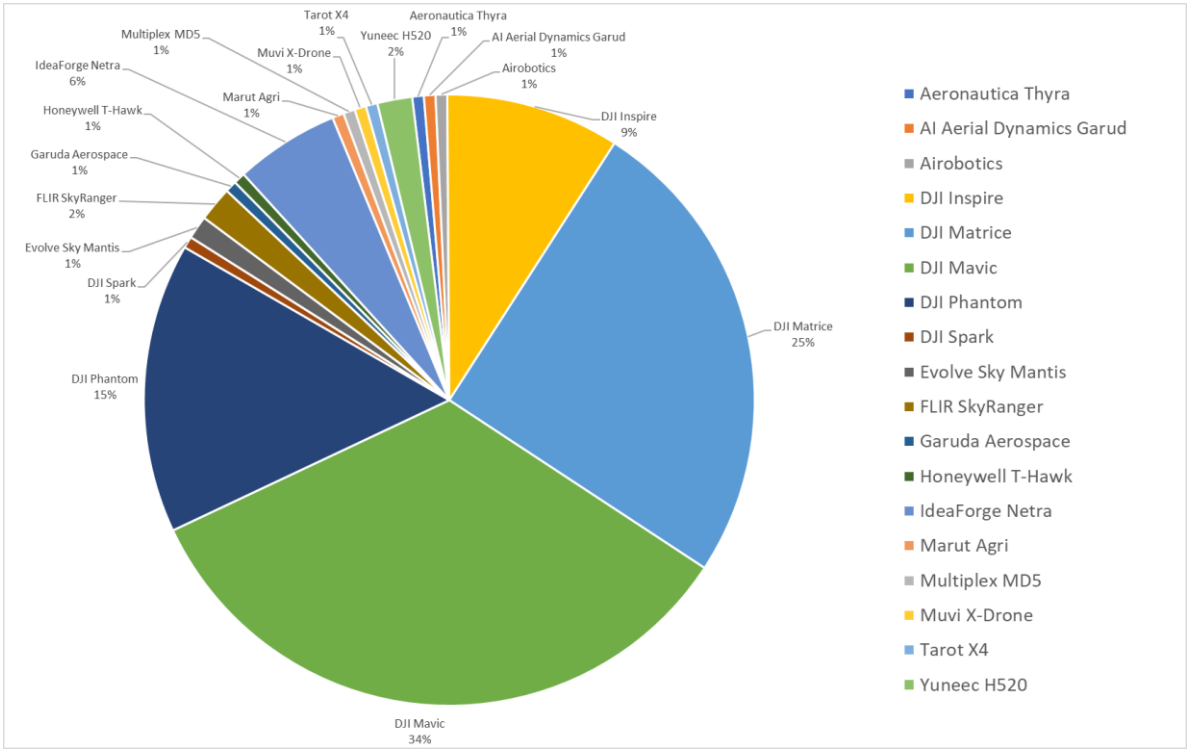


Figure 7: Percentage of Drone Utilised by Enforcement Agencies by Drone Model (Since January 2020)

That concludes our monthly roll up for the artefacts we have consolidated from January 2020 to May 2020. For more advanced statistics like these, get in touch with the team to find out what a Notify PLUS, PREMIUM or BUSINESS subscription can offer. You can get in touch with us a message at info@dronesec.com.

1.3. FEATURED ADVISORIES

The prioritisation table and its dependencies are explained in Appendix A, and relate to how we filter, analyse and visualise the intelligence we collect.

Intrusion and Trespass	Priority
Pakistan Army downs second Indian quadcopter in three days for intruding into border	**P2**

Summary

The Pakistani Army announced that they have shot down and recovered two quadcopters which infringed into their national boundaries.

Overview

In just over three days at two different locations, the Pakistani border Army spotted two separate DJI phantom quadcopters infringing into their borders. The first infringement saw a quadcopter entering 650m into Rakhchikri border and the second one intruded 700m into Kanzalwan border. These areas covered the Indian-Pakistan border and frequent drone incursions have occurred previously. The drones were seized; however, the drone operators were not located.


Analysis

The seized drones appear to be DJI Phantom 4 drones. The propellers in the second image appear to be the "Low-Noise" propellers sold by DJI (as seen by their aerodynamic design and 'flick' on the end), which claim to reduce up to 4dB (60%) of rotor engine noise. DroneSec has previously purchased and utilised these propellers for use in Red Team engagements where a discrete mission is required. While our experience is that they do not provide an extraordinary benefit over regular props, their use is certainly intended to be for missions seeking to decrease the possibility of attention.

Due to the low price-point of these DJI drones, it is possible that they were chosen and used as a one-way mission. In this case, forensic analysis of the drone's telemetry would be incredibly useful, potentially aiding in the launch location of the drone. It is important for law enforcement agencies to have a standard operating procedure (SOP) which aid to govern the process, people and methodology in taking down a drone and collecting forensic evidence of photos and videos stored within.

It is well known the conflict between India-Pakistan border groups and that Counter-UAV technology is in use at various points around the Indian side of the border. Both side record large numbers of drone incidents every month.

Tracked Actor Group:

India-Pakistan Border Drone Smugglers

Motivation and Goals:

- Use of unmanned systems as a battlefield tactical advantage;
- Use of unmanned systems to separate the distance and risk between operators and delivery payloads;
- Use of unmanned systems to conduct surveillance, reconnaissance and munition deliveries;

- Use of unmanned systems to overcome difficult physical terrain and personnel control barriers;

Tactics, techniques and procedures:

- Sourcing cheap and available Commercial-Off-The-Shelf (COTS) drones for one-way flights;
- Self-taught in unmanned and contraband-delivery UAS flights and operations;
- Recruiting local youths and elderly to conduct a significant number of regular border flights;
- Take-off and landing positions in close-proximity border villages and towns over Line-of-Control (LoC);
- Using small and medium-sized COTS drones to deliver munitions (grenades, mortars, small arms weaponry ~<15kgs) to guerrilla groups, often with purchased or home-made dropping mechanisms;

Recorded use of drone types:

- Quadcopters, Multi-rotors, Fixed-Wing

Recorded payload types:

- Ammunition, explosives, counterfeit money, firearms, communication devices, AK-47 assault rifles, grenades

Recorded member groups:

- Khalistan Zindabad Force (KZF) terror group
- Khalistani Jihadi Group
- Khalistani separatists
- Lashkar-e-Taiba
- Jaish-e-Mohammed

Contact DroneSec for a complete list of custom equipment used by this threat actor.

Recommendation

All incidents should be logged and categorised. Successful incidents often see offenders becoming lax with their approach and utilising the same take-off/landing points as before. However, as these drones were taken down, the Pakistani Army may expect offenders to take different paths of ingress to avoid detection. Event analysis from the drone data and video footages could assist in recognising patterns and trends (such as origin of flight, time of day etc.) providing possible modus operandi of the operator(s) and may aid in seizure on future attempts of incursions.

References:

https://www.thenews.com.pk/print/663976-pakistan-downs-indian-drone

https://www.dawn.com/news/1560204

https://store.dji.com/product/phantom-4-series-low-noise-propellers

Intrusion and Trespass	Priority
Drone intrusions over Darwen Moor fire grounds helicopters and hinders fire rescue efforts, UK	**P2**

Summary

Firefighters have been hindered in putting out the fire at Darwen Moor as helicopters are not able to fly due to sightings of drone operations.

Overview

The Lancashire Fire and Rescue Service were battling a fierce fire in Darwen Moor and engaged the use of helicopters to help extinguish the flame via airborne water drop. However, reports of drones flying overhead

the incident site restricted the entry of the helicopter into the Moor. The Fire and Rescue Service made a public announcement immediately requesting for public to keep their drones away from the area as it was actively hampering firefighting efforts. The drones were sighted but not seized and operators were not caught.

Analysis

It is now common to observe drone operators flying into restricted areas just to capture a snapshot of the 'action'. However, most of them do not have a full grasp of the scenes that are happening on the ground and the possible coordination of air movement during the event. Drone operators may not necessarily tune in to local civil aviation websites where Notice to Air Man (NOTAM) may have been issued, restricting the airspace from drone operations. Due to this ignorance, an increase in drone incursions have been happening globally, causing delays in emergency situations and bringing a negative impact on the drone industry.

Recommendation

For cases such as this, including medical evacuation where time is of the essence, it is important that these agencies have a drone management procedure with the local enforcement bodies. Simply producing a public announcement requesting operators to stop is often not enough to prevent it from reoccurring. Undertaking table-top simulations or exercises with local enforcement agencies to counter such scenarios aid to mitigate potential delays, overcome landing preventions and quickly involve the appropriate law enforcement bodies to remove the incursion.

DroneSec specialises in guiding organisations interested in procuring counter drone systems and setting up frameworks on drone incidence response. More information can be found at https://www.dronesec.com or email at info@dronesec.com.

References:

https://www.lancashiretelegraph.co.uk/news/18488435.helicopter-struggles-extinguish-darwen-moor-fire-due-person-flying-drone-incident/

Intrusion and Trespass	Priority
Three drone sightings near Glasgow Prestwick Airport, Scotland, UK	**P2**

Summary

Within 4 days, the Ayrshire Police logged three separate reports of drones flying near Prestwick Airport in Prestwick, UK.

Overview

Police from Scotland's Ayrshire division received calls on the sighting of drone operations near Prestwick Airport on three separate days. Although the drones did not cause any harm or mid-air collisions, they were treated with a potential risk of such a case happening. During this incident, neither the drone nor the operator was seized and apprehended; Prestwick Airport was not required to ground its fleet and halt operations.

Analysis

Drone operators must be cognisant of the laws set in place by their country, otherwise there could be a negative repercussion on the innovation within the drone industry as regulators enforce more stringent rules to clamp down on errant operators. Drone laws and no fly zones are set in place for safety reasons. A study from the FAA also concluded that drone strikes caused more damage to aircrafts and helicopters than bird strikes, due to the hard and rigid components of drones. With the capabilities of drones being able to fly further and higher, these advancements are beneficial when utilised correctly, but cause harm when not adhering to regulations set in place by authorities.

For specific threat actor intelligence pertaining to operators intruding airport space, please contact DroneSec.

Recommendation

Remote Identification and UAS Traffic Management (UTM) systems are a proactive approach to managing incidents between drones and manned aircraft. UTM systems enforce safe coexistence of unmanned and manned aircrafts, reducing the risk of safety infringements and potential loss of life.

In areas where counter-drone or drone detection systems are not readily available, having a drone management Standard Operating Procedure (SOP) or Incident Response Plan and undertaking table-top simulations or exercises to counter for scenarios like these are essential. Such training is also recommended for non-operators working in a field so everyone can play their part to mitigate drone incursions and the potential delays and loss of lives.

References:

https://www.heraldscotland.com/news/18488750.police-alerted-drone-sightings-prestwick-airports-restricted-airspace/

Intrusion and Trespass	Priority
Warning broadcasted for Odiham Airbase after drone sightings in vicinity increases, UK	**P2**

Summary

UK's Royal Air Force (RAF) Odiham Airbase saw an upsurge in drone operations within the vicinity and a public broadcast was made to inform operators of its illegality.

Overview

Despite having a restricted flight zone for the RAF's Odiham airbase, drone operations were still spotted within the vicinity. The RAF announced that it has seen an increase in number of drone operations within the area which pose a possible risk of mid-air collision with manned Chinook helicopters, which are the main asset of the airbase. The RAF made a public announcement to reiterate the laws of drones by the Civil Aviation Authority and reminded all public to abide by these laws.

Recommendation

Rules on drone operation can be found online in the local government aviation websites and mobile applications for the convenience of operators. Organisations with drone operations should aim to keep themselves and their personnel up to date and relevantly trained before operating a drone. It is the responsibility of drone operators to be sufficient trained, certified and updated with the latest regulations, procedures and NOTAMs as soon as they become available.

References:

https://www.basingstokegazette.co.uk/news/18486809.warning-increase-drone-usage-near-raf-odiham/

Intrusion and Trespass	Priority
Drone operator apprehended for flying over church in Chesterfield, England	**P3**

Summary

A drone operator flew over the town centre in Chesterfield allegedly due to the lack of people below.

Overview

Despite knowing that drones are not allowed to over congested areas without the correct permission, a drone operator chose to fly over his city town centre and a church given the lack of populace (due to COVID19). A tip off was made to the Derbyshire police and law enforcement officers were able to locate the operator and stop him from flying his drone. The operator claimed it was okay to fly his drone as the areas were quiet due to the pandemic movement lockdown. The police have since made a public broadcast announcing that flying over populace was not allowed without permission from the appropriate authorities – regardless of crowd count in

a congested area.

Analysis

Increasingly seen in drones, but common in typical police investigations, public community information can aid in the arrest of rogue drone operators. The help of the public as an eyewitness is beneficial for local enforcement agencies and these reports can be processed and logged to determine if the drone in case was similar to previous incidents. This evidence can lead to the discovery and arrest of persistent rogue drone operators.

With the rise in use cases of drones, more people are seeing the benefits of drones as part of their business activities or as a hobby. However, despite multiple public broadcasts on the rules for drone operations, there are still many users who fly drones into restricted areas due to ignorance or plain disregard of aviation laws. These acts have a negative effect on the drone industry and may see regulators enforcing more stringent rules affecting the legitimate and commercial drone operators more than the intended offenders.

Recommendation

While it may not be possible yet to provide city-wide coverage of drone detection and counter-drone systems, basic preparation measure can be set in place to respond to such incidents. A drone management plan and Standard Operating Procedure (SOP) should be drafted to govern the methodology in handling rogue drones. Enforcement agencies can also appeal to the help of the public as an eyewitness; it is beneficial to have a process for such evidence, and then carefully curated for collection and logging.

Organisations should also aim to undertake mock simulations to hone their response, improve communication flow between involved agencies and practice logging and monitoring of repeated cases. This practice can aid agencies in timing their response, mitigate risk and surface any challenges in communication and regulatory requirements.

References:

https://www.derbyshiretimes.co.uk/news/crime/drone-operator-dealt-derbyshire-police-after-flight-over-chesterfields-crooked-spire-church-2866673

1.4. NEWS AND EVENTS (P3)

Drone delivers contraband sparking 10-inmate brawl, system, weapons and narcotics seized

https://13wham.com/news/local/10-inmate-brawl-prompts-lockdown-at-auburn-correctional-facility

Multiple drone incidents over Prince Harry's residence in Hollywood Hills, California, USA

https://www.thedailybeast.com/prince-harry-and-meghan-markle-report-multiple-drone-flybys-to-lapd-will-now-pay-for-own-security

U.S. CBP flew unarmed Predator Combat-UAV in Minneapolis for protest surveillance mission

https://www.forbes.com/sites/krisholt/2020/05/29/cbp-predator-drone-minneapolis-george-floyd-aclu/#42d3d4c440fa

Kingpin of cross-border contraband drone delivery smuggling gang arrested, Punjab, India

https://www.news18.com/news/india/kingpin-of-gang-using-drones-for-smuggling-from-pakistan-nabbed-in-amritsar-2644101.html

Search and Rescue group's drone shot out of the sky, Sinaloa, Mexico

https://mexiconewsdaily.com/news/sinaloa-collectives-drone-shot-down-during-search-for-graves/

25 drones requested to monitor Malaysia-Thailand border to prevent illegal immigrants

https://www.thestar.com.my/news/nation/2020/06/01/malaysia-to-use-drones-to-monitor-border-with-thailand

Ukrainian military shoots down militant quadcopter drone in Marinka, Ukraine

https://www.mil.gov.ua/news/2020/05/28/shhodenne-zvedennya-pressluzhbi-minoboroni-ukraini-shhodo-obstanovki-v-rajoni-provedennya-operaczii-obednanih-sil/

Kent, UK police seek footage from drone flown by public that may contain evidence for murder

https://www.bbc.com/news/uk-england-kent-52860113

Two drones from Houthi terrorist group shot down in Yemen by Saudi coalition forces

https://www.al-monitor.com/pulse/originals/2020/06/saudi-yemen-intercept-houthi-drone.html

Night-time drone flights around neighbourhood potentially linked to robbery in Kildare, Ireland

https://www.dublinlive.ie/news/crime-drone-gardai-breakingnews-theft-18321494

1.5. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P3)

Indonesian Citizens reminded to seek approval from Civil Aviation Authority and Police for drone flights during Movement Control Order (MCO)

https://www.sabahnewstoday.com/cmco-public-must-have-caam-permit-to-fly-a-drone-ismail-sabri/?lang=en

How Basil Hassan Launched Islamic State Terror into the Skies

https://ctc.usma.edu/the-controller-how-basil-hassan-launched-islamic-state-terror-into-the-skies/

Evolution of UAVs employed by Houthi forces in Yemen (Update)

https://storymaps.arcgis.com/stories/46283842630243379f0504ece90a821f

Swarms of mass destruction: Declaring armed and autonomous drones as WMD (commentary)

https://mwi.usma.edu/swarms-mass-destruction-case-declaring-armed-fully-autonomous-drone-swarms-wmd/

https://www.airuniversity.af.edu/Portals/10/CSDS/monographs/MONO60%20Drone%20Swarms%20as%20WMD.pdf?ver=2020-05-13-135901-057 (PDF Document)

US Army's new drone swarm may be a weapon of mass destruction (commentary)

https://www.forbes.com/sites/davidhambling/2020/06/01/why-new-us-armys-tank-killing-drone-swarm-may-be-a-weapon-of-mass-destruction/#6a10b2e3ece8

Adapt or Die: Command Posts – Surviving the Future Fight (commentary)

https://www.dvidshub.net/news/370818/adapt-die-command-posts-surviving-future-fight

Case Study: Las Vegas – Drone Detection in Action

https://www.911security.com/blog/case-study-las-vegas-drone-detection-in-action

1.6. COUNTER-DRONE SYSTEMS (P4)

DroneALERT launches V2.0 incident drone reporting and intelligence system

https://www.drone-detectives.com/main/

Dedrone partner with BlackBerry to deploy advanced alerting capabilities within their C-UAS

https://www.dedrone.com/press/dedrone-and-blackberry-partner-to-counter-unauthorized-drone-activity

AMS Defence sign with Blighter Surveillance for C-UAS systems for Australian deployment

https://www.defenceconnect.com.au/key-enablers/6204-major-win-for-sovereign-integrator

US Marine Corps Systems Command seeking C-UAS systems and organisations

https://www.dsjournal.com/2020/05/27/marine-corps-systems-command-marcorsyscom-seeks-to-identify-c-uas-sources/

https://beta.sam.gov/opp/a1ffd7a65eb0415d845f7e6496cfa1ae/view

Bristol airport implements Clearsky drone detection and threat management system, UK

https://www.aviationpros.com/airports/airport-technology/press-release/21140044/telent-telent-and-dgs-installing-worldclass-antidrone-system-at-major-uk-airport

Meteksan Defence releases anti-jamming product capable of detecting and supressing jamming signals using spatial filtering

https://www.meteksan.com/en/news/anti-jamming-gnss

No clear answers on how to effectively detect, mitigate drone threats (commentary)

https://www.aviationtoday.com/2020/05/27/no-clear-answers-on-how-to-effectively-detect-mitigate-drone-threats/

1.7. INFORMATIONAL (P4)

Police cars and headquarters command control room to link with drone camera, Sircilla, India

https://telanganatoday.com/sircilla-cops-link-drones-with-patrol-cars

Teal drones release details of their down-selected Army's Short Range Reconnaissance Program

https://tealdrones.com/

Drone manufacturer VINVELI pivots from farming drone to armed, weaponised 'Vero' drone

https://liteye.com/farming-drone-goes-from-plowshares-to-grenade-launcher/

Minot PD engaged SkySkopes to search for missing child, North Dakota, USA

https://www.verizon.com/about/news/how-missing-child-was-found-help-drones

Irvine police find arsonist through the use of drone, Irvine, California, USA

https://www.ocregister.com/2020/05/29/22-year-old-arson-suspect-found-by-irvine-police-drone-arrested/

Matrice 200 drones deployed in Kenya to catch citizens flouting movement restriction, Africa

https://www.the-star.co.ke/counties/central/2020-05-30-police-use-drones-to-nab-those-escaping-lockdown/

U.S. Border Patrol drone team finds 3 illegal immigrants lost in Anza-Borrego desert

https://www.cbp.gov/newsroom/local-media-release/new-drone-program-assists-rescue-one-woman-and-two-teenage-girls

Papua New Guinea to receive 28 Phantom drones from ADF for border surveillance

https://www.rnz.co.nz/international/pacific-news/417801/drones-to-help-patrol-png-border

Nottinghamshire police drone unit release statistics on law enforcement use over past 6 months

https://westbridgfordwire.com/police-drones/

Oslo police start using drones around the capital for emergency use, Norway

https://www.aftenposten.no/osloby/i/LAwEzp/Oslo-politiet-tester-utrykning-til-oppdrag-med-droner-fra-fredag

Myrtle Beach police department release drone team footage of protest walks, USA

https://wpde.com/news/local/myrtle-beach-police-release-drone-footage-of-sundays-protest-walk-to-plyler-park

US Army launch first flight of Martin UAV V-Bat, Fort Campbell, Kentucky

http://www.airrecognition.com/index.php/news/defense-aviation-news/2020/june/6290-us-army-launched-the-first-flight-of-martin-uav-v-bat.html

1.8. SOCIAL (P4)

Drone surveillance footage of looting during George Floyd protests in Chicago, USA

https://twitter.com/jeffcolon/status/1267300199946428418

https://twitter.com/CounterVulture/status/1267290320221474816

Drone aftermath footage of George Floyd protests in USA

https://www.youtube.com/watch?v=htcU0V-g9L4 (Minneapolis, Minnesota)

https://www.youtube.com/watch?v=yueae28J_6U (Minneapolis, Minnesota)

https://www.youtube.com/watch?v=p--HwBn2CFQ (Los Angeles, California)

https://twitter.com/ebphil2/status/1267893606871904256 (Richmond, Virginia)

Drone Attacks against Critical Infrastructure: A Real and Present Threat (Video)

https://www.youtube.com/watch?v=b_n9XH4RtP8

Gwent Police Department conduct several serious investigations using drones, Wales UK

https://twitter.com/GPRuralCrime/status/1268113052131614720?s=20

DOJ Guidance for Counter-UAS Technology and What It Means for Site Security

https://twitter.com/SIAonline/status/1267112607384829952?s=20

Spying on America Part 2 – Protecting Data on Drones (webinar)

https://www.youtube.com/watch?v=3uI4NeT8guk

World of Drones and Robotics Congress opens for abstract submissions for Brisbane, Australia

https://www.worldofdrones.com.au/submit-abstract

DJI AirWorks conference 2020 changes from in-person to virtual event

https://enterprise-insights.dji.com/blog/airworks-goes-virtual

Israeli drone spotted flying over GAZA

https://twitter.com/IsraelGazaICN/status/1267802029331582977?s=20

1.9. DRONE TECHNOLOGY (P5)

SoarTech wins bid to develop AI unmanned fighter to fight alongside with manned jets

https://www.militaryaerospace.com/defense-executive/article/14176812/artificial-intelligence-ai-dogfighting-unmanned

Researchers use commercial drones with infrared camera for automated landmine detection

https://techxplore.com/news/2020-05-drones-machine-dangerous-butterfly-landmines.html

Flying Taxi, Ehang, gets approval to test delivery of 150kg cargo load

https://asiatimes.com/2020/06/ehang-eyes-heavy-lift-cargo-drones/

QinetiQ Australia selected to design and construct UAS Flight Test Range in Queensland, Australia

https://aaus.org.au/qinetiqftr/

https://aaous.wildapricot.org/resources/Documents/UAS%20FTR%20FactSheet.pdf (PDF)

APPENDIX A: THREAT NOTIFICATION MATRIX

A.1. OBJECTIVES

The sole focus of this service is to supply organisations with key evidence, alerts and intelligence relating to (1) Drones, (2) Counter-UAS and (3) Universal Traffic Management (UTM) systems. Together, these three items are referred to as: **DCU**. This intelligence provides a defensive net for early warning systems, fine-tuning systems based on trends and providing agencies with factual evidence in support of selecting or rejecting the need for counter-solutions. High priority will be given for the following artefacts:

- Unfolding situations or incidents relating to DCU;
- Private or public-based vulnerabilities, exploits or attack vectors affecting DCU;
- Global or national regulatory changes affecting DCU;
- Remarkable vendor or brand-specific news releases.

If an artefact is released that is considered the highest priority level (P1), Notify customers will receive an email alert linking them to the intelligence details located within their Notify portal account.

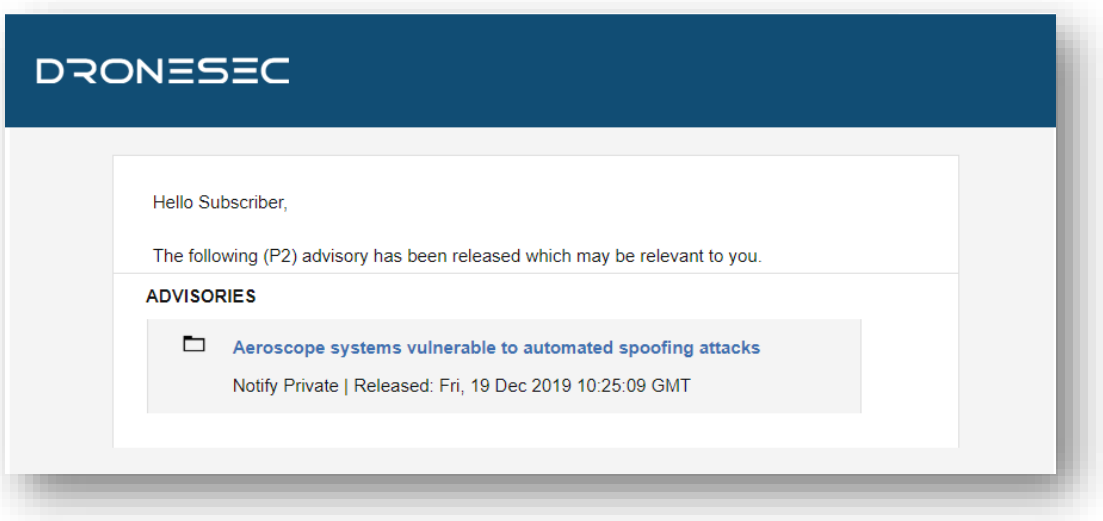


Figure 8 - A threat notification specific to a Notify customer's listed keywords.

DroneSec uses a methodology to rank, prioritise and filter intelligence pieces. This rating merges threat intelligence standards with the type of source (public, private, underground) and affected system (DCU).

Threat notifications are prioritised based on the following table:

Priority Level	Description
P1	Directly specific to a Notify customer
P2	High importance incident or situation
P3	Medium importance event or information
P4	Low interest or general news/media
P5	No direct evidence, market trends or informational

In general, (P1) alerts will only be visible to the affected customer to protect their privacy and general information security. However, abstract (P1) information will at times be shared with other Notify customers. Priority levels are often highly contentious as it requires understanding of a customer's environment, context and what might be deemed 'actionable' for them. The added spanner in the works is that DCU is made up of cyber-physical systems – there are traditional security vulnerabilities, physical and kinetic risks and even privacy, regulatory and aviation considerations in play. As a result, we set the priority level based on a number of key metrics that are very specific to our Notify customers; the more information provided about an entity, the higher the quality-gate of prioritisation we apply to our filter process.

Associated with each artefact of intelligence, you'll find a set of tags. These tags are used for indexing, searching and quickly visualising if the information is relevant to your organisation. As with any system, ours will continue to better itself as it learns more about the various artefacts that are most important to our customers, and their types of environments and systems. You'll find the tags, and examples of them, in the tables below.

There are three categories we focus on. We do not extend past these, as to keep our intelligence relevant and brief.

Tag - Categories	Description
Drones	Custom-made or Commercial-Off-The-Shelf (COTS) systems that might: • Be known as UAS[1], UAV[2], RPAS[3]… • Weigh 50g all the way to 250kgs • Are automated or manually piloted • Have associated devices, software or infrastructure
CUAS	Counter-UAS systems that might: • Be known as Counter-Drone or C-UAV

[1] UAS: Unmanned Aerial System
[2] UAV: Unmanned Aerial Vehicle
[3] RPAS: Remotely Piloted Aerial System

	• Detect and/or respond to drones • Be standalone, hand-held, static or integrated with a UTM[4] or PSIM[5] system • Have associated systems, software, infrastructure and communication protocols
UTM	Universal Traffic Management system that might: • Be known as Urban Air Mobility (UAM) or fleet management systems • Manage, track, communicate with or interdict drones and/or drone swarms • Be software and/or hardware based • Have associated systems, software, infrastructure and communication protocols

Within DCU, there are many areas of concern. For those in a position of ingesting Threat Intelligence, these are the key concerns we have determined are relevant for the information we collect.

Tag – Areas of Concern	Description
Cyber Security	Technical attack vectors, risks, threats, vulnerabilities, guides, OSINT[6], exploits or zero-days[7]. This may also contain confidentiality, Privacy, Integrity and data sovereignty artefacts
Safety	Safety concerns related to assets, environments, persons or critical systems as a direct result of the artefact. This can be caused by physical, kinetic or electronic sources.
Regulatory	Global or national law or regulatory-based amendments, announcements or ordinance that affect DCU.

Sometimes the artefacts may cover a range of sectors. For organisations looking to filter out noise, this is a key tag that will help provide insight into their chosen sectors.

Tag – Affected Sector	Description
Residential	Houses, suburban areas and private property.
Commercial	Cities, major working areas and buildings

[4] UTM – Universal Traffic Management System
[5] PSIM – Physical Security Information Management System
[6] OSINT: Open-Source Intelligence from the public domain.
[7] Zero-day: Otherwise known as an 0day or unknown, unpatched vulnerability of which the vendor does not yet know exists.

Government	Government-managed locations
Critical Infrastructure & Security	Water, energy, docks, airports, prisons, transport, stadiums and military
All Sectors	The above sectors, combined

APPENDIX B: SOURCES & LIMITATIONS

B.1. INTELLIGENCE SOURCES

DroneSec uses a variety of government, military, law enforcement, vendor and citizen-based intelligence sources. Not all of these sources are public. Sources or artefacts that cannot be verified by a third-party are clearly marked.

Source Name	Description	Intelligence Type
International Aviation Authorities	Aviation authorities are the regulatory bodies for managing air and drone activities within a range of jurisdictions. Their level of access includes pilot, airport, airprox and public incident reports.	Statistics Incidents
Academic Sources & University Agreements	Keyword alerts on various academic portals and research agreements with Higher Education provide Notify with the latest journals and papers with a focus on DCU.	Research Papers Studies and Reports
Pilots – Commercial and Private Airlines	Pilots currently active in the commercial or private airline industry.	AirProx Reports Visual Identification Reports
Commercial Partnerships	Our partners in the military defence, commercial vendor and security industry exchange intelligence with Notify.	Statistics Incidents Sentiment and chatter Vulnerabilities and Exploits
Counter-UAS vendors	Counter-UAS vendors with multiple systems in place around the globe. Their systems detect, record and (where allowed) react to malicious drones. Detection telemetry data is shared with Notify.	API and manually provided statistics
DroneSec Research	The DroneSec team conducts penetration tests, vulnerability analysis, aerial threat simulations and forensics on a variety of DCU which results in zero-day intelligence of various systems. Whilst respecting the privacy of our clients, statistics and agreed information is shared with Notify.	Incidents Whitepapers Research Papers Vulnerabilities and Exploits Open-Source Intelligence
Deep, dark and surface web communication channels	Groups, message boards and forums dedicated to modding and bypassing common drones and counter-drone controls. DroneSec actively participate and contribute in these forums to better understand the threats and risks relevant to our clients.	Manual and automated analysis based on keywords and word-clouds.
Information Security Sources	A variety of public and private sources within the Information	Vulnerabilities and Exploits Incidents

	Security, threat intelligence and Open-Source Intelligence (OSINT) communities provide Notify with recent, actionable information.	Whitepapers Research Papers Sentiment and Chatter
Newsletters and Email Lists	A variety of commercial (paid) and public sources. Gated content is exchanged with Notify within a strict agreement basis. Good examples of public sources include the Center for Study of the Drone (Bard College).	News Incidents Studies and Reports
Law Enforcement	Notify collects information from public, private and Freedom of Information (FOI) portals from Law Enforcement and shares combined metrics back to agencies.	Events Incidents Statistics
Proprietary aggregation software - Search Engines - Social Media - Government Sources	The DroneSec Notify secret sauce. Our aggregators, dorks, scripts and macros receive, filter and analyse DCU-related data, filtering for relevant and actionable information.	News Events Incidents Whitepapers Research Papers Sentiment and Chatter
Subscribers & Individuals	Subscribers of dronesec.xyz, dronesec.com and individual contacts provide manual reports to the Notify service. Contact us to see how exchanging Threat Intelligence could provide additional support to your organisation.	Incidents Research Papers Sentiment and Chatter

B.2. LIMITATIONS

Intelligence gathering reflects a point-in-time notification and/or analysis in-scope objectives (DCU). Future changes to the artefacts and the availability of new information could introduce retraction of statements or alter the wording, ratings and analysis of artefacts outlined within this report.

While DroneSec conducts in-depth fact-checking and evidence-based analysis of the information, sources and events, we aggregate information that may not be proven to be factual. Wherever possible, we try to mark this as such. DroneSec pushes for quality over quantity – but understands the needs for a broad approach to intelligence within DCU. Not all Notify reports will include analysis; delivery is subject to time the Intelligence is detected and its availability at time of Notify release.

Another limitation to the report is the lack of introductory material for a new reader to the DCU space. While news events, situations and analysis can help, newcomers to the industry can get in touch with us at info@dronesec.com or via the slack channel to seek additional clarification on topics, phrases or informational courses that might uplift their knowledge and understanding in the area.