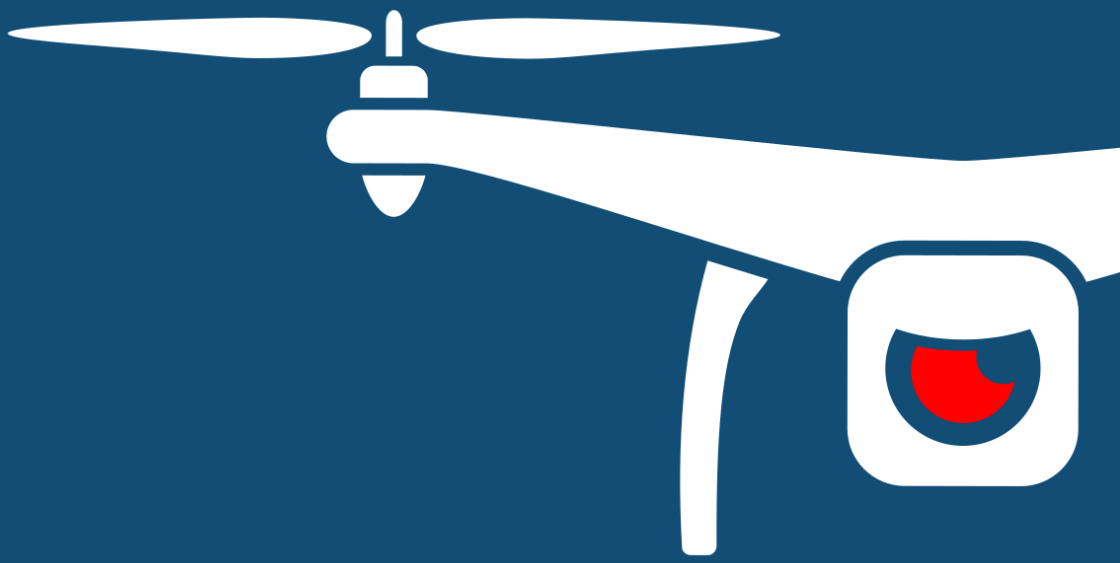
DRONE SEC
A Privasec COMPANY

NOTIFY ISSUE #21

WEEKLY THREAT INTELLIGENCE

06 May 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

Welcome to another monthly roll up of our public Threat Intelligence release. We'll go through some of the more interesting statistics we've observed during the month gone (April). Many of these artefacts help us make certain estimations and determinations about the future – more on that later though, as we'll be adding some drone security 'predictions' to our State of Drone Security report in June.

We appreciate all Notify artefacts provided via community submissions; notably for the Digital Forensic tool Autopsy's newest Drone Analyzer ingest module. You'll find this, and a number of featured reports, all within this week's Threat Intelligence report. You may also see some contact information provided in the featured recommendations too; that's because our team is highly skilled and able to provide remediation services in these areas.

This week, I want to deconstruct how our database catalogues and visualises 'artefacts' provided in reports such as these. So, what goes into an artefact? For example, you might only see the following:

-

Illegal drone flies over jockey race, operator found caught by security personnel, Hong Kong

https://www.scmp.com/sport/racing/article/3082659/drone-operator-faces-legal-action-after-flying-over-sha-tin-racecourse

-

In reality, the backend take-away is much more complex (and useful). Our Drone Security Analysts combine Open-Source Intelligence (OSINT), Imagery Intelligence (IMINT) and Geo-spatial Intelligence (GEOINT) to categorise, classify and assess drone incidents. Big acronyms, but they all serve a purpose.

When our threat intelligence team receives a notification or observes an incident, it is triaged and logged with a number of identifiers. This is then be used to geo-locate the incident on a map, compared to other incidents that didn't result in an arrest, and identify patterns that might suggest if the operator has been involved in drone incidents before (yes, we log names of individuals and groups where Law Enforcement have been involved in drone incidents – and where this information has been made public).

Item	Description	Result
Time & Date	Seventh Race, Sunday 3rd May	Exact HH:MM time that the incident occurred: **3:37pm** https://www.racenet.com.au/horse-racing-results/sha-tin-20200503/norman-conqueror-hcp-c4-race-7
Location	Sha Tin racecourse, Hong Kong	Exact geolocation where the incident occurred, matching photographic evidence with satellite images/maps: **22°24'02.6"N 114°12'23.0"E** **22.400713, 114.206375**
Visual Item	A picture and video that show the drone.	Confirmation of the make and model of the drone. Exact location of the drone, part of its flight direction and angle.
Statement	Operator location and pattern recognition. *"Jockey Club security were able to take a photo of the operator on the far side of the nearby Shing Mun River and send it to police, who swiftly responded."*	Provides a geo-location radius of the possible take-off and landing areas around the Shing Mun River – capped by the drone model's maximum flight operational range. This can feed into future SOPs.

Statement:	Operator location and pattern recognition. *"It is not the first instance of a drone above the track this season with an incident also occurring at Happy Valley."*	Useful information in potential repeated drone infringements. Follow up lead on identifying if the same make and model were in use.
Incident or Use	Classifier of what type of incident it was for statistics, grouping and categorisations.	In this case, it was an incident. Use is simply where a Police Force uses a drone for an action. An incident involves rogue or malicious use of a drone.
Apprehension, seizure or getaway	Classifier of what type of incident it was for statistics, grouping and categorisations.	In this case, it did result in an apprehension. This is a useful statistic as it helps map police and crime figures of the number of incidents resulting in apprehension vs those that got away. Necessary for program uplift and feedback. Seizure is for when a drone is seized but the operator escapes (or not located). Getaway governs any incident that does not result in apprehension or seizure, albeit an incident.

Now that the information is logged, we can do very quick and powerful searches to receive unique insights. For example, if someone searched for queries requesting drone incidents that:

- Occurred in Hong Kong
- Resulted in Arrest
- During May 1st – May 10th

They would find any incidents that matched, including the above horse racing incident. Because of the information logged, the indicators of both can be analysed to see if any patterns exist. Coupled with other sources (law enforcement, drone detection systems, UTM systems, keywords) this information provides a pre-fact and post-fact enumeration tool for drone activity. This moves Law Enforcement closer to identifying repeat offenders where individuals or groups are intentionally misusing drones.

I hope you find the above useful in the effort that goes into each artefact, and the incredible use of which can be extracted from it. For more information on our Notify Threat Intelligence Platform and what it could do you for organisation, please feel free to chat to the team at info@dronesec.com.

- *Mike Monnik, DroneSec CTO*

TABLE OF **CONTENTS**

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 May, 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, six hundred and forty artefacts were recorded which roughly equates to 5.3 drone security incidents/events **per day.** The number of events logged has increased significantly in the past two months mainly due to the widespread use of drone to monitor and restriction movement of citizens globally in an attempt to curb the spread of COVID-19. The use of drones complemented the efforts of local law enforcement agencies by first using drones to survey with the likes of thermal cameras, then apprehending offenders with boots on the ground.

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	174	5.6	30 (20.11%)
April	192	6.4	18 (9.38%)
Total (2020)	**640**	**5.3**	N/A

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 April 2020: Notify release #4 – #20.

We see a huge jump in News and Events on drone utilisation as well as Whitepapers and Publications on drones. Both increments are somewhat linked during this period as we see more organisations and government agencies welcoming the use of drone deliveries for medical supplies or basic necessities during the controlled movement restriction order in place. Within the local neighbourhood, drone hobbyists use the technology to deliver toilet paper to their relatives or purchase food from a market. On the larger scale of things, drone deliveries serve to improve the quality of life for families who are badly affected by the lockdown. Hence, regulations around the world have been relaxed for Beyond Visual Line of Sight (BVLOS) drone operations as deliveries sometimes can span across tens of kilometres (some across straits and isles) before arriving at their destination.

Category	Number of Artefacts (Jan - Apr 2020)	Number of Artefacts (Jan - Mar 2020)
Featured	25	19
Cyber and Information Security	13	10
News and Events	181	135
Whitepapers and Publications	109	78
Counter-Drone Systems	58	51
UTM Systems	30	17
Drone Technology	67	63

One key metric we use is priority level – this is explained in our Appendix but means that an artefact (determined by category) can change priority based on our matrix. For that reason, it can be insightful to gauge how we align evidence of events to perceived organisational priority and risk. Below you will find a breakdown of how many artefacts were reported in each priority tier. As with any security threat modelling, it is difficult to ascertain risk without knowing what an organisation deems important in their unique environment. As a company, we try to prioritise specifics (e.g. keywords provided by a customer) over unknowns to filter out noise and ensure notifications do not include 'SPAM'.

April 2020 saw a significant increase in number of P3 and P5 artefacts due to the widespread use of drone technology around the world. Drones are utilised to control and restrict movement, spread public message to citizens and to disinfect/sanitise cities. In addition, we also see an uptick in number of cases of drones utilised to send contraband into prisons, or intruding airspace illegally.

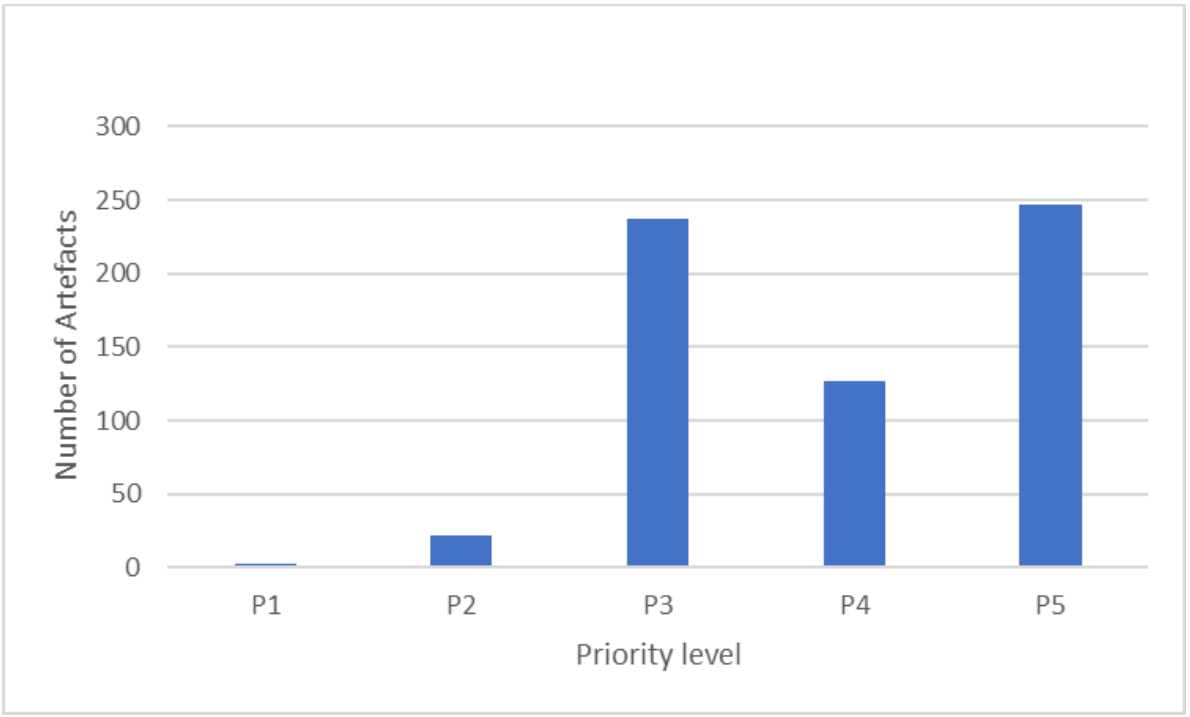


Figure 1: Number of Artefacts by Priority Levels (Since January 2020)

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. April 2020 saw an increase in number of drone-drops within prisons, usually drugs or firearms. 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.

Recently, in issue #18, we saw guidance from the USA Attorney General on better protecting facilities with counter drone solutions and highlighting the importance of law enforcement agencies acting on this guidance urgently. 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 flow and processes required for drone incidents.

Critical infrastructure facilities such as power and energy, prisons, and territorial borders with frequent incursions as 'hotspots' should prioritise the development of counter-drone measures to guard against rogue drones.

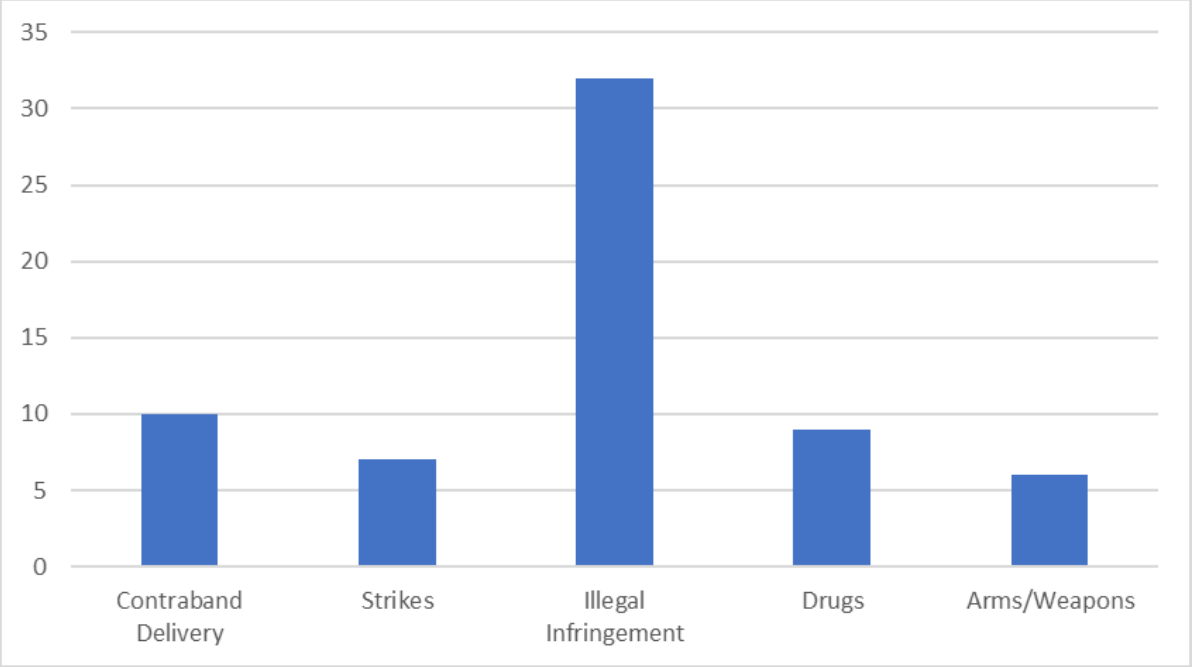


Figure 2: Number of Drones Utilised by Category of Activities (Since January 2020)

-

DroneSec records the locations and countries where drone incidents occurr. In April 2020, we see more drone infringements happening at prisons, residential neighbourhoods and hospitals as compared to March 2020. There were several artefacts on attempted contraband deliveries via drone-drops within prisons. Drones are still positioned as a relatively safe method of committing illegal

activities, due to the lack of law enforcement strategies and separation of the operator from their device.

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.

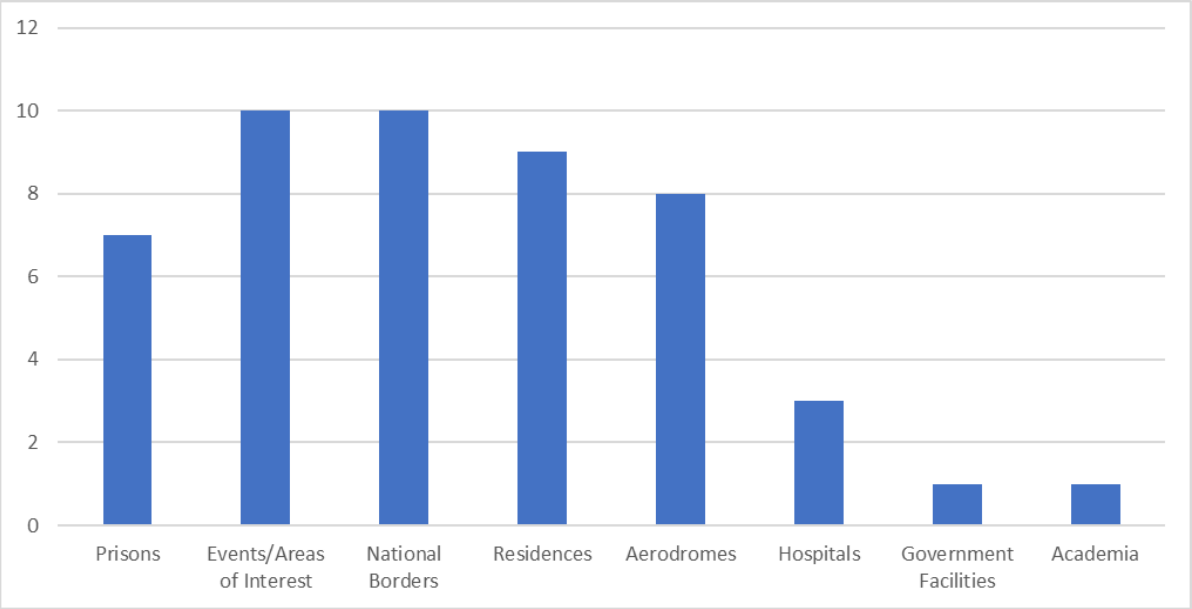


Figure 3: Number of Drone Incidents by Location of Occurrence (since January 2020)

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:

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 lockdown measures during COVID-19 or arrest hiding criminals, (2) government agencies and organisations – to check on vast areas of facilities or environment or medical deliveries, and also into (3) commercial and hobbyist lifestyles such drone lighting visual aerial displays, technological research and advancement, or deliveries of food and/or essentials.

Countries with early adopters and implementation of drones have had an increase in discussions around drone regulations during COVID19. Adhering to these principals 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.

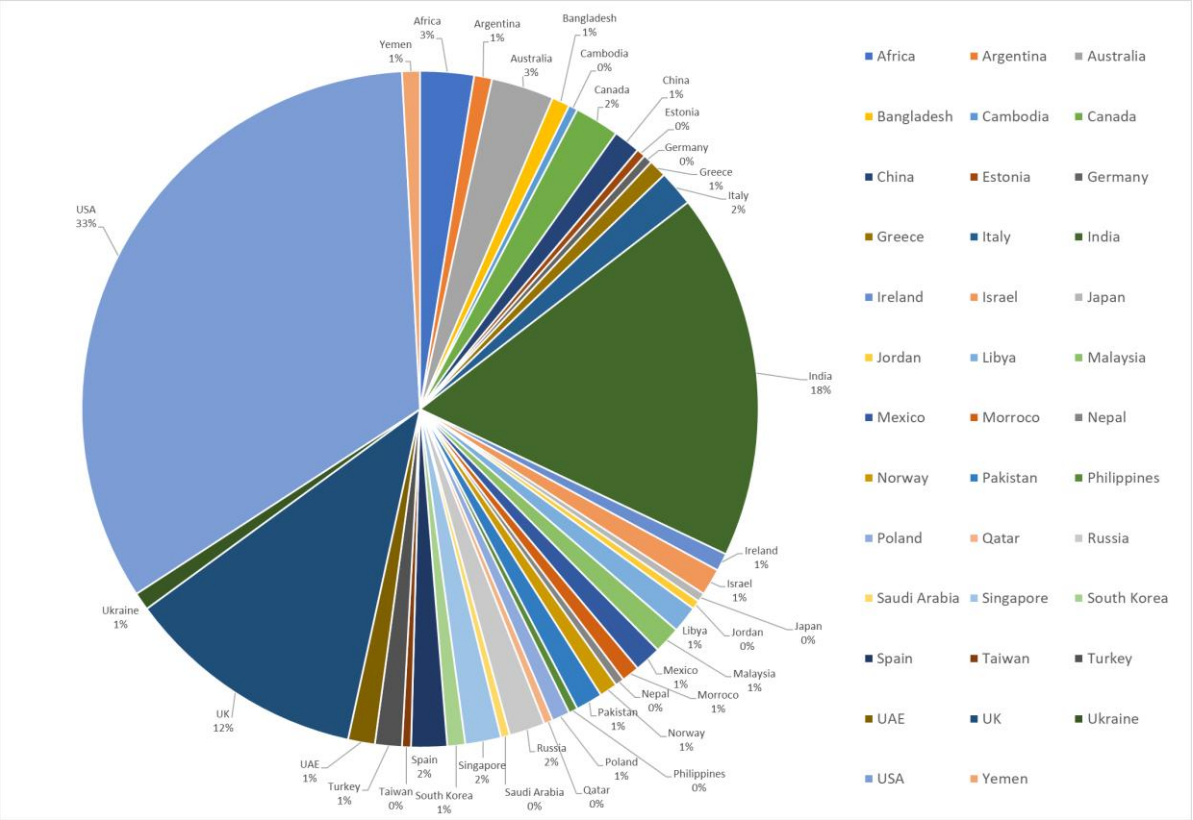


Figure 4: Percentage of Drone Artefacts by Country of Occurrence (Since January 2020)

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 drone 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, continually develops drones that are able to fall within global guidelines and regulations (size, weight, remote identification).

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.

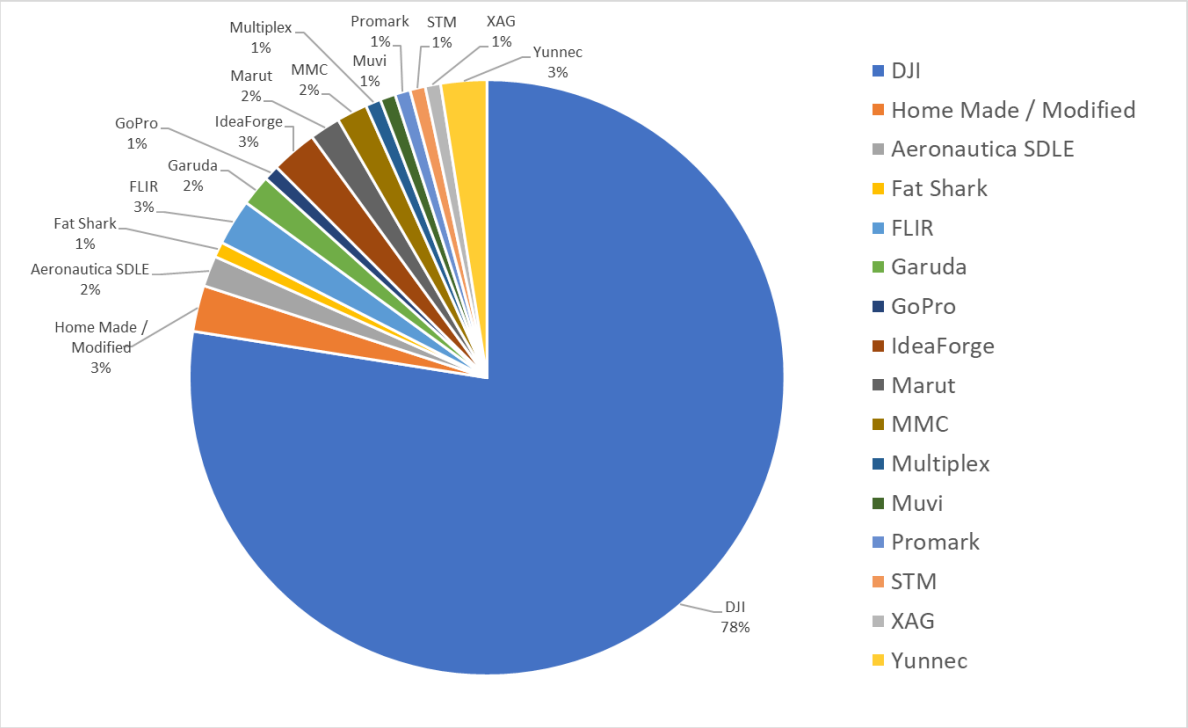


Figure 5: Percentage of Brands of Drones Utilised (Since January 2020)

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.

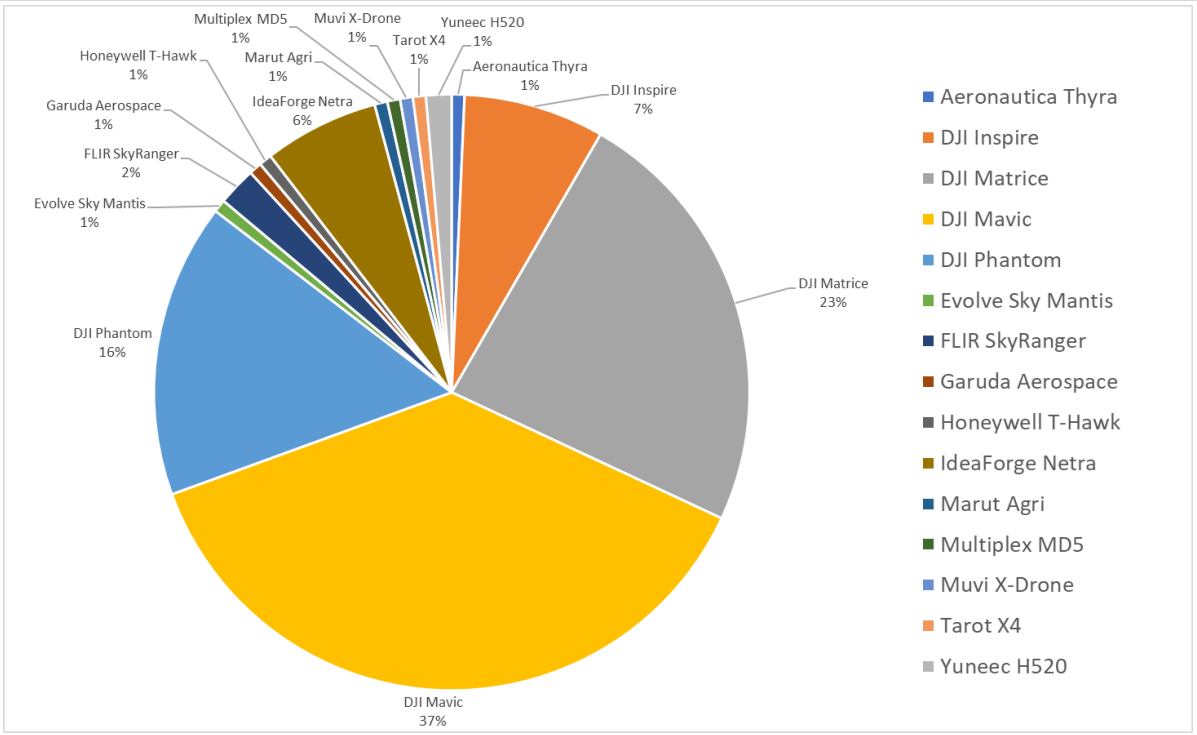


Figure 6: Percentage of Drone Utilised by Enforcement Agencies by Drone Model (Since January 2020)

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

1.3. FEATURED ADVISORIES (P2)

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

Safety and Security	Tags	Priority
2 Inspire and 1 Phantom DJI drones found fitted with explosives	Drones, Safety, Modding, Explosives, Cartel, Security, Rogue Drone, Apprehension, Mexico	P2

Summary

During a raid on three stash houses in Mexico, authorities found three drones modified with external electronic devices to carry and trigger C-4 explosives and other homemade bombs.

Overview

In an anonymous tip given to the Office of Mexico's Attorney General, local authorities in San Andres Cholula, Puebla, Mexico, were authorised with a search warrant to raid three houses for items which could lead to acts of terror as part of an organised crime syndicate. In the search, authorities found three DJI drones, two Inspire 1 models and one Phantom 3 model modified with an electronic board and wires capable of carrying and trigger explosives. Several other C-4 explosives, gunpowder, homemade explosives devices, weapons, ammunitions, and communication equipment were also found.

Analysis

The first major publicity of drones being used to drop explosive payloads was during skirmishes against the Islamic State, ISIS. However, outside of war combat situations, drones have been used for border reconnaissance and maliciously in the 2018 Caracas drone attack against the President of Venezuela. However, this is one of the first times we see drug cartels or organised crime syndicates using similar methods (explosive payloads) by drones instead of just reconnaissance or contraband drops.

Using payload-capable drones is a cost-effective and risk-reduced technique without being spotted and allows operators to distance themselves from the immediate blast radius. Drones allow malicious users to operate safely with a low risk of being apprehended by law enforcement agencies due to being disconnected from the threat. In addition, these small sized drones can hover in air for a long time at a high altitude, giving it an advantage to stay hidden until it used to drop the explosive ordinance.

Operating the drone itself has a low skill barrier, however, in this situation, there is some operator experience and domain knowledge required. For example, the syndicate had to build a printed circuit board assembly to work in tandem with the drone on releasing the explosives. Offenders for such acts tend to get away easily as

many common public areas do not possess drone detection or counter drone systems to mitigate the threat.

Recommendation

DroneSec recommends all local law enforcement agencies to be prepared and ready for such threats. 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 threat management plan and Standard Operating Procedure (SOP) should be drafted to govern the process, people and methodology in handling a drone threat.

Organisations should also aim to undertake mock simulations in reacting to such payload drone incidents to hone their response, improve communication flow between emergency and rescue agencies and practice on the logging and monitoring of repeated cases. This information can aid law enforcement agencies in practicing and timing their response, mitigate risk and undergoing challenges faced in communication and regulatory requirements.

In the event of an eyewitness, it is beneficial to have a process for, and then carefully collect evidence for collection and logging. This data can help to determine if the drone was similar to previous cases which may help provide the modus operandi of rogue groups and assist in the arrest of the operator.

DroneSec offers services in guiding organisations interested in procuring counter drone systems, drone threat intelligence within their environment, setting up frameworks on drone incidence response, or simply educating on drone operations and security. More information can be found at https://www.dronesec.com or email at info@dronesec.com.

References

- https://www.breitbart.com/border/2020/05/05/drones-outfitted-with-explosives-seized-in-mexico-in-active-terrorism-investigation/

Exploits and Vulnerabilities	Tags	Priority
Riga Airport closed due to a lost and uncontrolled drone	Drones, Safety, Commercial, Airport, Uncontrolled, Riga Airport	P2

Summary

During a controlled test flight at Riga Airport in Latvia, a drone was pronounced uncontrollable and lost communication with the operators.

Overview

SIA UAVFactory was conducting a flight test at Riga Airport, Latvia, when communication between the aircraft and the ground control station was broken. The drone was allegedly meant to have automatic engine shut-off when communication links are lost, however, this did not occur during the incident. The aircraft, of about 3.5 meters by 5.5 meters, weighs 26 kilograms and was last commanded to fly at a certain altitude and in an orbit before it was lost. There has been no news of the missing aircraft since and operators are still trying to regain communication control with the drone in order to locate it. As the drone had fuel sufficient for 90 hours of flight time, Riga Airport had to divert all incoming aircraft below 19,500ft and close the airport to avoid any potential mid-air collision with the drone.

Analysis

Most drones operate on wireless frequencies, of which the channels and range can be shared by other devices. Although larger classes of drones that are mainly used in the military have their own protected channel to avoid 'sharing' with others, it is still possible for a loss of signal and communication link to occur. Interference can be caused by many reasons such as jamming or even a malfunctioning hardware. However, in cases like these, all drones nowadays have a "Loss of Link" procedure which commands the aircraft to perform a series of actions such as returning and landing at its take-off point or flying to a marked location and spiralling downwards until it crash lands.

In several cases, these drones might actually continue in their last commanded direction, instead of simply

engaging the "Loss of Link" procedure – this is because the last command could be repeated continuously within the malfunctioning system, or the drone is within a looping pre-programmed flight. This does put the system in a bit of a spin and some interesting results are revealed which should add to the knowledge base of operators so that such unexpected use case can be avoided. This is similar to conducting a 'de-authentication' attack via a Wi-Fi based drone; it will often continue in its navigated path.

While little is revealed about the system of the drone, some manufacturers have hardcoded a "Return Home" programme within the drone which commands the drone to return back to the manufacturer's designated crash landing site when all other commanded programmes fail. Without this knowledge, operators might think that the drone is operating in an uncommanded manner. However, it is necessary to know that all drones will only perform actions based on input or pre-programmed chain of commands.

Recommendations

It is recommended that drone operators have a good understanding on the capabilities of their drones –the intricate command functions available in the drone in every possible scenario, flight time, range and protocols or frequencies in use. Practice of the worst-case scenario (Red Team and War Room scenarios) happening and work backwards to ensure you and your team have appropriate controls. These are important details which aid operators in planning their pre-flight mission and handling ad-hoc changes when unexpected contingencies may occur mid-flight.

In the event something like this occurs, the crew should also have a forensic or incident response kit ready and waiting to collect the evidence, hardware and software data to piece together the story of what happened. Logging on both the drone, controllers and interconnected systems/software should provide enough telemetry data to discern what is accidental link-failure, bird strike or operator mistake over a malicious de-authentication attack, signal jam or protocol manipulation of the devices.

It is always recommended to select a (drone and control link) brand that has been independently tested from a security and penetration testing point of view, conduct a simulation catering for malicious individuals targeting the event for mitigation and remediation purposes. This is something DroneSec provides as a core speciality – please contact info@dronesec.com to enquire about Red Teaming and Aerial Threat Simulation services.

References:

- https://www.apollo.lv/6964378/noskaidrotas-jaunas-detalas-par-pazuduso-dronu
- https://www.theregister.co.uk/2020/05/04/latvian_drone_breaks_free/

Exploits and Vulnerabilities	Tags	Priority
Drone intrusion into Nanaimo Airport, Vancouver	Drones, Safety, Commercial, Airport, Infringement, Nanaimo Airport	P2

Summary

A drone was spotted at altitude by a commercial pilot on approach into Nanaimo Airport in Vancouver, Canada.

Overview

During the approach to Nanaimo Airport in Vancouver, Canada, a pilot spotted a black, small to medium sized commercial drone just off its left wing. Almost at the same altitude to the aircraft, the pilot felt that the drone was too close to the approach path of the aircraft and reported the incident. There was no operational impact to the flight and the manned aircraft landed successfully. However, neither the drone nor the drone operator was found after the incident.

Analysis

It is now fairly common to observe drones flying into restricted areas due to ignorance or disregard of aviation law governing drone flights by drone operators. Despite public broadcast on what can and cannot be legally undertaken with drones, there are still many operators who continue to disregard these for a variety of

reasons. However, this instead has a negative effect on the innovation within the drone industry as regulators will enforce more stringent rules to clamp down on these errant operators – sometimes, affecting the legitimate and commercial drone operators more than the intended party.

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. These materials when ingested flew much deeper into the engine and dealt a greater proportion of damage compared to birds. With the capabilities of drones being able to fly further and higher, some allowing operators to fly the drone beyond visual line of sight (BVLOS). these advancements are beneficial when utilised correctly, but cause harm when not adhering to regulations set in place by authorities.

Recommendation

Unmanned Traffic Management (UTM) systems are a proactive approach to managing incidents between drones and manned aircraft – when the flight is not intentionally malicious. UTM systems enforce safe coexistence of unmanned and manned aircrafts, reducing the risk of safety infringements and potential loss of life due to medical aviation delays. Drone operators should be cognisant with the laws of their country and have the appropriate licenses if required. Operators should aim to keep themselves up to date or relevantly trained before operating a drone.

For law enforcement and medical aviation bodies where counter-drone systems are not readily available, undertaking table-top simulations or exercises to counter for scenarios like these are essential. Training is recommended for non-operators working in a field that could be affected (both directly and indirectly) by rogue or disruptive drones. Furthermore, organisations should have a Standard Operating Procedure (SOP) or Incident Response Plan in play to mitigate potential delays, overcome landing preventions and quickly involve the appropriate law enforcement bodies.

DroneSec offers services in guiding organisations interested in procuring counter drone systems, monitoring drone threat intelligence within their environment, setting up frameworks on drone incident response, or simply educating seasoned and newcomers with training courses on drone operations and security. More information can be found at https://www.dronesec.com or email at info@dronesec.com.

References:

- https://www.nanaimobulletin.com/news/rcmp-notified-after-drone-comes-too-close-to-plane-landing-at-nanaimo-airport/

Security	Tags	Priority
2 of 3 drones recovered in an attempted drug smuggling via drone drop	Drones, Infringement, Contraband, Borders	P2

Summary

Yuma Sector Border Patrol agents intercepted three attempted drop packages containing drugs in 5 days.

Overview

Over a period of 5 days from April 29th to May 3rd, 2020, Yuma Sector Border Patrol intercepted 3 attempted drone drops across the USA-Mexico border. The patrol agents recovered over 11kg in dropped packages with drugs in them at a street value of more than $300,000 USD. The drones were launched during the cover of the night, however, the border patrol agents managed to seize two of the three drones that were used for the contraband delivery. As investigation were still ongoing, no further details on the drones used we released – DroneSec will be releasing the make and models as soon as these are made available. It is unknown what type of drones, payload-weight capacity or flight time the drones were capable of.

Analysis

This is a very clear case of smuggling via a drone drop-off by a repeating offender or organised group. Although not disclosed, the drones used are likely easily available with a sufficiently low price point. Using the drone as a transportation tool to conduct illegal acts presents the offender with low risk of being apprehended as drones and the controller by separated by distance. Furthermore, the skill barrier to be able to fly a drone is

not complex, allowing such methods to be widely used by drug smugglers.

Recommendation

Yuma Sector Border Patrol likely have a drone security management plan in place. Drones were not only spotted but were also taken down thereafter. However, due to the low price-point of drones, it is possible these were 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 handling a drone, collecting evidence and responding to potential operators in a pre-determined radius around the protected grounds.

Likewise, all incident 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. Hence, event analysis from the drone data and footages can help to determine if the drone was similar to previous cases and/or took similar launch/land flight paths. Monitoring the drone make and models, and recognising patterns and trends (such as origin of flight, time of day etc) may help provide the modus operandi of rogue groups and may aid in the arrest of the operator. This information can aid law enforcement agencies in practicing and timing their response, undergoing challenges faced in communication and regulatory requirements, and providing stakeholders with assurance to risk planning and mitigation.

Finally, protected facilities that are in counter drone denied environments (whether regulatory or financially) should seek detection systems that do not seek to necessarily mitigate but do provide tracking and post-incident analysis capabilities.

DroneSec offers services in guiding organisations interested in procuring counter drone systems, monitoring drone threat intelligence within their environment, 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.cbp.gov/newsroom/local-media-release/yuma-sector-agents-intercept-narcotics-dropped-drones-0
- https://twitter.com/USBPChiefYUM/status/1257440896720809987

1.4. NEWS AND EVENTS (P3)

Illegal drone flies over jockey race, operator found caught by security personnel, Hong Kong

https://www.scmp.com/sport/racing/article/3082659/drone-operator-faces-legal-action-after-flying-over-sha-tin-racecourse

Ukrainian soldier wounded from grenade dropped by drone

https://www.unian.info/war/donbas-war-ukrainian-soldier-wounded-as-enemy-drops-grenade-from-uav-10981814.html

Popular Digital Forensics tool 'Autopsy' adds Drone Analyzer ingest modules for DJI

https://www.autopsy.com/autopsy-4-15-release-highlights/

Woman in Lone Tree, USA, lodges multiple reports of drone flying outside apartment

https://kdvr.com/news/lone-tree-woman-concerned-about-drone-flying-near-apartment-complex/

Nottingham, UK Police 'drone team' use drones to locate car thief suspect

https://www.nottinghampost.com/news/nottingham-news/no-escape-police-drone-finds-4098383

Lancashire, UK Police 'Tactical Operations Drone Team' arrest wanted man hiding on rooftop

https://www.lancashiretelegraph.co.uk/news/18423224.drone-spied-man-hiding-roof-mystery-accomplice/

Harris County and SWAT operators deploy drone to catch mail fraud and counterfeit ringleader

https://www.coveringkaty.com/news/drone-used-by-precinct-5-deputies-to-catch-suspect/article_b82bb328-8e2f-11ea-ac94-c7f4c3fabe15.html

Civil Rights Group in the USA raise privacy concerns on CVOID19 drone use by law enforcements

https://www.usatoday.com/story/news/politics/2020/05/03/coronavirus-police-use-drones-enforcement-privacy-concerns/3059073001/

French Human Rights League files complaint against drone use over video storage concerns

https://news.bloomberglaw.com/privacy-and-data-security/paris-cop-drones-spark-covid-19-privacy-backlash

Israel Ministry of Defence purchases loitering exploding drone for tactical edge in close combat

https://www.upi.com/Defense-News/2020/05/04/Israel-Defense-Ministry-buys-small-exploding-drones/1961588616741/

1.5. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P3)

FAA announces training initiative to support academia in drone education and skills development

https://www.faa.gov/news/updates/?newsId=95432

Barbados extends suspension on importation and licensing of drones to October 2020

https://gisbarbados.gov.bb/blog/ban-on-drones-extended-for-six-months/

FAA select ResilienX to develop Contingency Management Platform for its UTM BAA program

https://www.resilienx.com/faa-funds-contingency-management-powered-by-resilienx-fraihmwork

Drone Forensic Investigation: DJI Spark Drone as A Case Study

https://www.sciencedirect.com/science/article/pii/S1877050919315625?pes=vor (PDF Document)

Drone Attacks Against Critical Infrastructure: A Real and Present Threat

https://www.atlanticcouncil.org/wp-content/uploads/2020/05/DRONE-ATTACK-0420-WEB.pdf (PDF Document)

Indian government eases restrictions on drone use for COVID-19 initiatives

https://indicanews.com/2020/05/04/india-eases-restriction-to-use-drones-launched-gaurd-to-fight-covid-19-pandemic/

https://www.civilaviation.gov.in/sites/default/files/Public%20notice_GARUD_Exemptions%20for%20Covid-19_2%20May%202020.pdf (PDF Document)

1.6. COUNTER-DRONE SYSTEMS (P4)

How the Justice Department is permitted to use Counter-Drone technology (Commentary)

https://www.nextgov.com/emerging-tech/2020/04/how-justice-department-permitted-use-counter-drone-technology/165047/

The use of drones by nation state missions highlighted as a threat to country by Netherlands Military Intelligence and Security Service, new counter-terrorism division dedicated to drones

https://www.defensie.nl/downloads/jaarverslagen/2020/04/30/jaarverslag-mivd

https://www.defensie.nl/binaries/defensie/documenten/jaarverslagen/2020/04/30/jaarverslag-mivd/web_4_MIVD_Openbaar+jaarverslag+2019.pdf (PDF Document)

1.7. UTM SYSTEMS (P4)

Altitude Angel launches API to allow sharing and receiving of flight data in near real-time

https://www.altitudeangel.com/news/posts/2020/may/altitude-angel-launches-surveillance-api/

1.8. DRONE TECHNOLOGY (P5)

Russia National Guard deploys drones and helicopters to enforce lockdown measures

https://www.dailymail.co.uk/news/article-8282265/Russia-suffers-record-rise-10-633-new-cases-fresh-infections-country-Europe.html

136 drone light show by Verge Aero in Philadelphia to thank medical workers

https://www.inquirer.com/health/coronavirus/coronavirus-philadelphia-penn-drone-light-show-verge-aero-covid-19-20200430.html

https://www.facebook.com/mandi.specos/videos/10163573646545357/

300 drones light the skies in Rotterdam Netherlands dedicated to healthcare workers

https://www.dezeen.com/2020/05/05/studio-drift-franchise-freedom-live-stream-vdf/

Liloan, Philippines, partners with Mataverse to deploy 10 drones to enhance COVID measures

https://www.manilatimes.net/2020/05/04/public-square/liloan-launches-drones-to-combat-the-pandemic/722335/

Merida City Hall and DJI Merida launch "Stay Home" campaign with Inspire drone, Mexico

https://www.theyucatantimes.com/2020/05/merida-city-hall-has-launched-stay-home-campaign-using-drones/

Aerodyne clocks 1,000 flights with 40,000km covered while assisting in COVID-19 lockdown order

https://www.geospatialworld.net/csr-initiatives/aerodyne-drones-completes-1000-flight-hours-in-covid-19-operations/

Entrants continue submissions in US Air Force Agility Prime eVTOL program

https://www.janes.com/article/95784/companies-unveil-offerings-for-us-air-force-s-agility-prime-evtol-effort#.Xqw_Qh7fBBA.linkedin

1.9. INFORMATIONAL (P5)

Drone operator locates missing boy with FLIR-enabled drone after 7-hour search, USA

https://www.brainerddispatch.com/news/6461927-Extensive-search-finds-missing-11-year-old-boy

Drones used to search for missing hiker who fell into water, Meadville, Pennsylvania, USA

https://triblive.com/local/regional/dogs-drone-and-more-than-50-volunteers-still-searching-for-meadville-man-missing-at-mcconnells-mill/

Savannah PD, USA, uses drone to aid in fire investigation

https://www.wsav.com/crime-safety/early-morning-fire-at-city-of-savannah-code-compliance-building-under-investigation/

Fairfield PD, USA, uses drones to monitor social distancing at beaches, wary of citizen's concerns

https://www.fairfieldcitizenonline.com/news/coronavirus/article/Fairfield-police-use-drones-to-monitor-social-15246344.php#photo-19374612

Goa Police, India, to start using drones to monitor citizens in slums during lockdown

https://www.deccanherald.com/national/coronavirus-goa-police-use-drones-to-monitor-lockdown-violators-833284.html

Delhi Police employ drones to ensure social distancing within queues at wholesale markets

https://www.aninews.in/news/national/general-news/delhi-police-use-drones-for-surveillance-in-ghazipur-market20200504112305/

Clovis Police in Fresno, California USA trial a 90-day drone pilot program for incident response

https://www.yourcentralvalley.com/news/clovis-police-now-using-drones-when-responding-to-emergency-calls/

AI drones to aid cultural heritage sites in monitoring and investigation, Seoul, Korea

http://koreabizwire.com/cultural-heritage-administration-to-deploy-drones-for-safety-management/158460

How drones could kill a US destroyer warship (Commentary)

https://liteye.com/how-drones-could-mission-kill-a-u-s-destroyer/

1.10. SOCIAL (P3)

DJI M200 tethered drones were used by NFL security teams during the 53rd US Super Bowl event

https://www.youtube.com/watch?v=SEOuKHeh6ck

Antioch Police Department, USA, use Mavic II Enterprise Zoom to arrest stolen vehicle subject

https://www.linkedin.com/posts/rick-smith-298376199_antiochpd-nopursuit-evidence-activity-6662726201020420096-_H3t (Video)

Antioch Police Department, USA, use drone to detain armed group

https://www.linkedin.com/posts/rick-smith-298376199_drone-officersafety-publicsafety-activity-6662547967075057664-KF2Q

Arcturus UAV providing VTOL and payload capacity advantages to US army

https://www.linkedin.com/posts/philipmahill_army-activity-6663108697142759424-_sdP

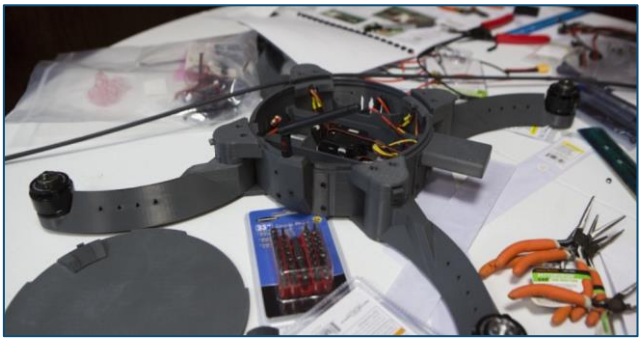
Downed reconnaissance drone in Herat

https://twitter.com/medows_xyz/status/1257015950928343040

Building and programming your own quadcopter from scratch

https://www.youtube.com/watch?v=XEvDYOs060E

https://interestingengineering.com/diy-drone-learn-how-to-build-your-own-quadcopter-drone



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.

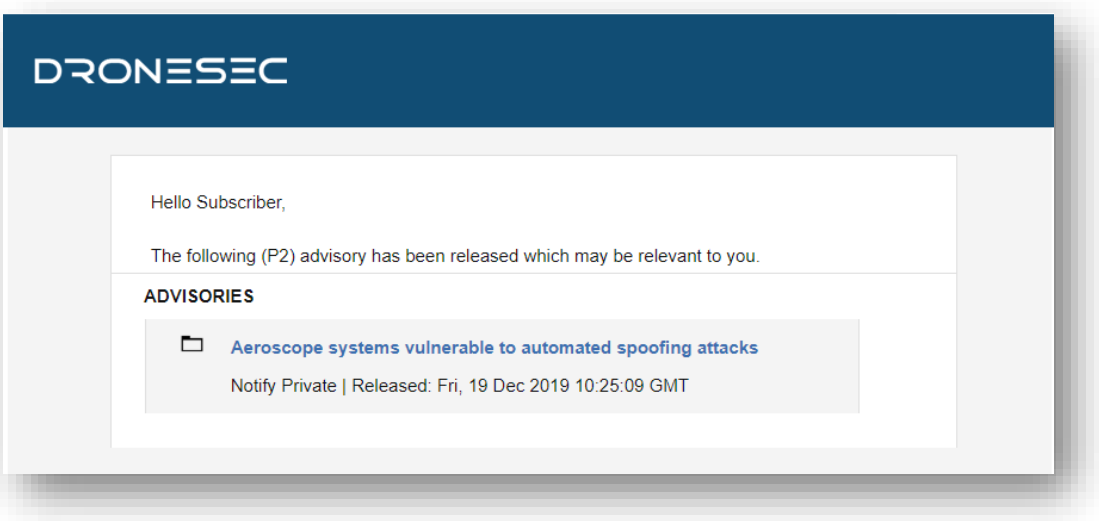


Figure 7 - A threat notification specific to a Notify customer's listed keywords.

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.