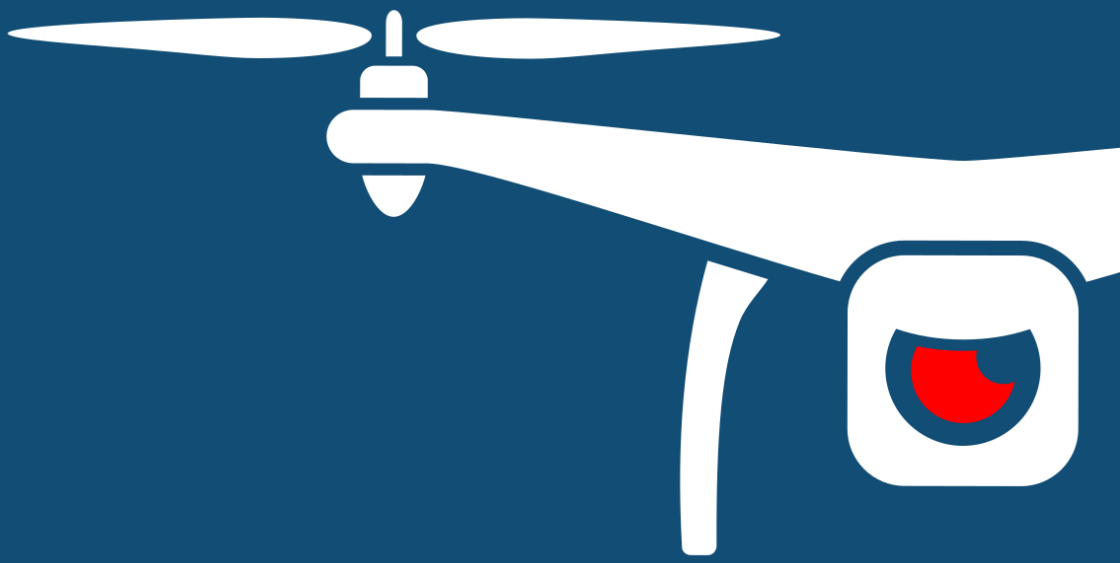
DRONE SEC
A Privasec COMPANY

NOTIFY ISSUE #29 (PUBLIC)

WEEKLY THREAT INTELLIGENCE

01 July 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

This week we see the launch of the Parrot ANAFI USA drone, really pushing a number of security-centric features such as on-board encryption, anti-theft and data transmission security features. Fundamentally, it features a 'made in USA' heritage and was initially built for DoD / Law Enforcement. The next six months will be a critical time period for the DJI x Parrot tussle, as we see many DJI Matrice 300 contracts being fulfilled across the country but with the obvious data security and privacy conversation ongoing. We will be keeping a lookout for technical security analysis of the system and will undertake our own as soon as they are made available.

In other news this week, the US Army has announced the Counter-Drone systems that have met its selection criteria, producing a number of well known and also not-so-well known contenders. Meanwhile, the US National Transportation Safety Board has produced a very detailed report on an aviation incident covering a drone collision with a helicopter. Great read, thought-out methodology and is peppered with quality images and visual guides – a must read for anyone who might have a similar role to play elsewhere in the world.

DJI launch a drone rescue map to visualise drone intervention within rescue operations (many of these can be found in our database) and are part of our recording of 'law enforcement use of drones'. It is a great looking, interesting dynamic and consistent with their shift to supporting and highlighting the use of UAS within first responder use.

Free user access will be available on the DroneSec Notify platform from tomorrow (02/07/2020).

Just a reminder that from tomorrow, we will be opening up the platform to FREE tier users – this means you can receive artefacts and updates via the platform and search our database. The limitations of course, are that you will not receive:

- Access to the Knowledge Base
- Featured (P2) or Unique (P1) incident reports
- Tracked Assets and Keywords via the Monitoring Engine

This is a terrific expansion to our regular weekly PDF offering, and we hope you'll enjoy it. You will continue to receive the Weekly public threat intel emails, just like this. For more information on what features are offered to the FREE tier, please click here.

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

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 July, 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 paid members via the DroneSec Notify 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.

Notice to our readers: our monthly roll-ups and featured advisories will cease to be publicly available as DroneSec Notify moves to the online platform. Both content have provided context and field-based learnings to important issues. However, with the ever-growing database that we have, DroneSec has moved onto an online repository where artefacts and reports can be tracked, classified and analysed much easier. Featured analysis from now on are more comprehensive, wider in spectrum but only available on the Notify platform.

-

In 2020 thus far, one thousand and sixty-four artefacts were recorded which roughly equates to 5.84 drone security incidents/events **per day.** The number of events logged has increased steadily in the past few months mainly due to the increasing number of organisations (military, law enforcement, federal and commercial) gearing towards the utilisation, regulation and innovation of drones and its ecosystem.

This being said, we are actively modifying our data to ensure that *incidents* and *everything else* are categorised adequately; there is a growing need to observe only threats compared to that of the business intelligence we include with all issues. In future roll-up's, you will find the number of incidents per day separate to events, news and other non-incident information.

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%)
June	219	7.9	19 (8.68%)
Total (2020)	**1064**	**5.84**	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 June 2020: Notify release #4 – #28.

We see a 18% increase in whitepapers and publications in the month of June 2020. Most of the publications were focused on drone technology, the proliferation of drones in the Middle East and how to counter against drone attacks in today' society. Drones have been used extensively in the Middle East by rebel troops and terror groups, targeting civilian and military key installations. While drones are beneficial towards enforcement agencies and commercial owners, crime syndicates have also found themselves a new tool to conduct their nefarious activities.

Category	Number of Artefacts (Jan - Jun 2020)	Number of Artefacts (Jan - May 2020)
Featured	61	46
Cyber and Information Security	21	18
News and Events	240	217
Whitepapers and Publications	163	133
Counter-Drone Systems	86	71
UTM Systems	47	39
Drone Technology	105	89

-

DroneSec has collected, tagged and logged several key statistics for the year 2020 and in our mid-year review of 2020, we will be focusing on the collated drone incidents we have recorded thus far.

We saw cases of drone utility and innovation such as UAS Traffic Management (UTM) and SATCOM technologies rising globally, we are also seeing a rise in number of incidents that are related to drones. At DroneSec, we classify drone incidents as events where drones were used as a medium in the conduct of illicit acts. Events where drones were used for the transportation of weapons, narcotics and/or contraband across borders or restricted areas are classified as drone incidents. Similarly, events where drones were sighted to have infringed airspace boundaries of manned aircrafts or areas with no-fly-zones such as hospitals or airports are also classified as drone incidents.

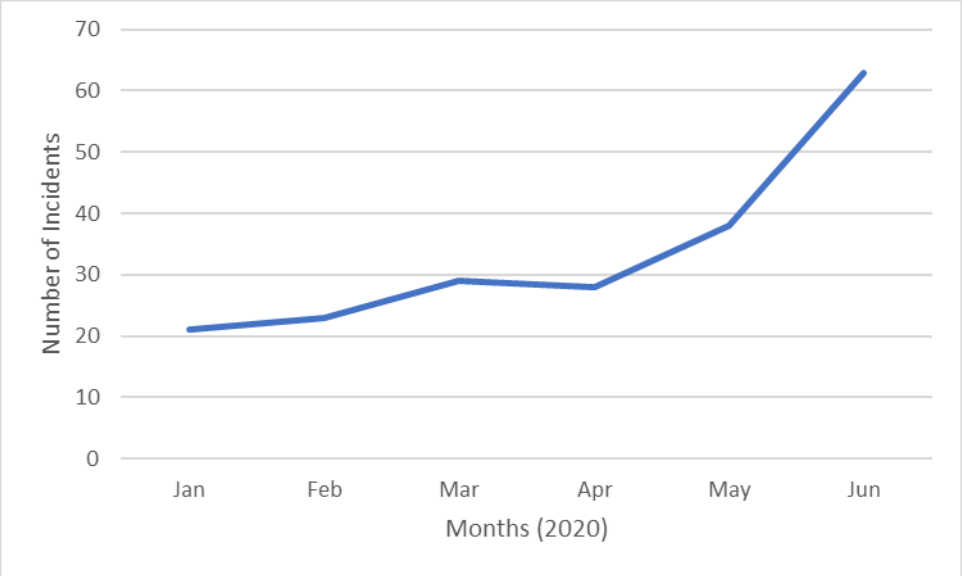


Figure 1: Number of Drone Incidents for the Year 2020

Drone incidents rose sharply in the month of May 2020 and June 2020 as we see a huge jump in drone deliveries into prisons and across borders. Organised crime syndicates may have spent the 2-months lockdown period during March and April 2020 to consolidate and innovate their methodologies in conducting crimes. Drones have proven to be cheap, effective and easily available. In addition, drone operations provide natural separation between the drone operator and the area of transaction, allowing multiple attempts without the risk of being apprehended.

From all the drone incidents that were recorded, DroneSec saw that only 57% of the drones sighted were seized by law enforcement agencies, either by firing (with traditional calibre ammunition guns) or that the drones had crashed or were stuck in trees. Of the remaining 43%, most of the drones were sighted and not found thereafter. Some key installations are 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. DroneSec recommends for these areas to start looking into a drone management plan. A basic plan would serve to help create processes and workflows when an incursion happens. Without one, rogue drone operators will only continue to be more brazen with their operations and possibly increase the amount of damage done to the facility.

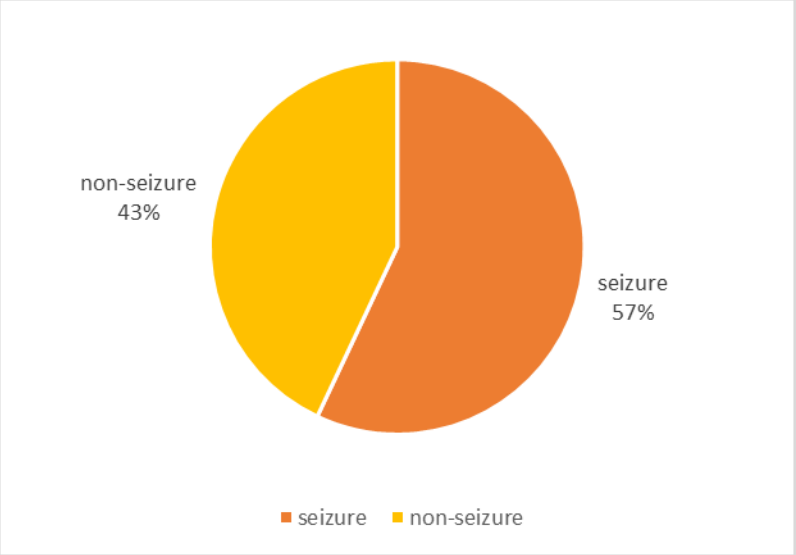


Figure 2: Percentage of drone incidents where the drone system was seized

Not surprisingly, only 25% of rogue drone operators were apprehended for their illicit act(s). Not only are drones small and versatile in escaping from the detection of law enforcement agencies, it creates a distance between the operator and the area of operations. Nefarious operators will use this to their advantage and flout drone laws to conduct their illegal activities as risk of apprehension is reduced. Law enforcement agencies who have seized drones should also request for digital forensic analysis on the data stored within the drones. Important information such as flight details, time of journey, take off locations and images and video footages of the environment and operator's face may be evident within. This information will help to bridge the gap in tracing and arresting the offender.

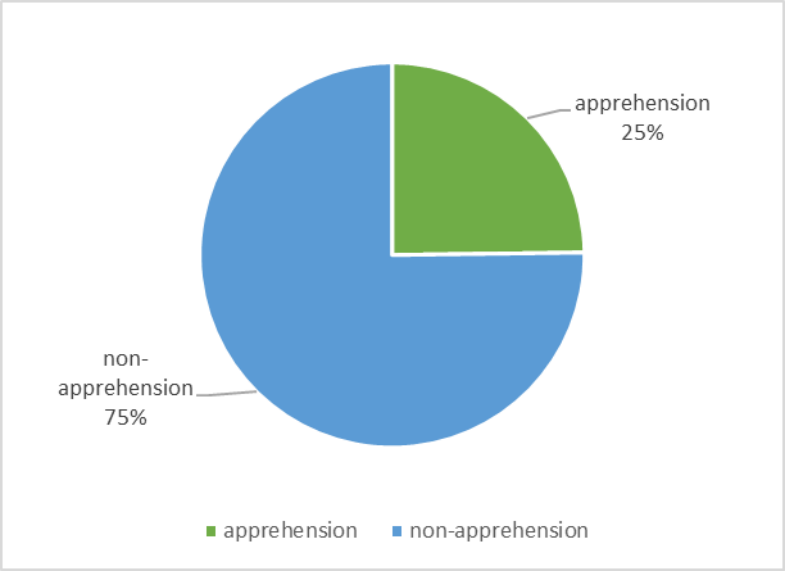


Figure 3: Percentage of drone incidents where the drone operator was apprehended

-

Continuing on, we've gathered some of the key metrics around specific events where drones were 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 the law and an increase in the number of cases involving illegal infringements and contraband deliveries.

June 2020 saw a large spike in number of drone infringement across borders in the Middle East and East Asia. DroneSec advocates for borders security forces to adopt procedures relating to drone incidents if counter drone systems are not economically feasible or permissible. Critical infrastructure facilities and areas such as prisons and territorial borders with frequent incursions should prioritise the development of counter-drone measures to guard against rogue drones. However, much of this feasibility 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 drone incursions. Procurement of counter drone systems may be required to undergo a lengthy process due to the extensive staff work within the government bureaucracy and critical infrastructure may only start seeing positive effects months or years later.

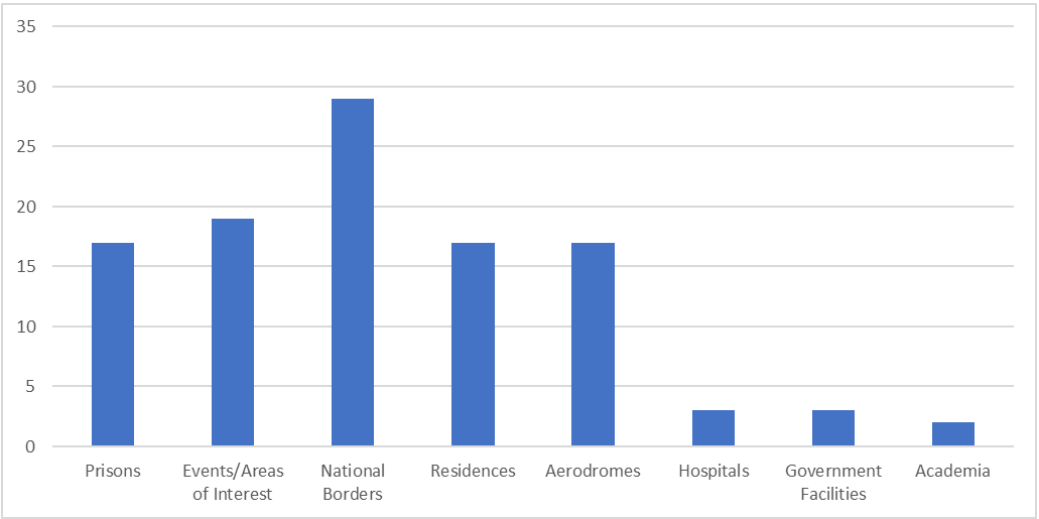


Figure 4: Number of Drone Incidents by Location of Occurrence (since January 2020)

In the meantime, security forces can take the effort to carry out tabletop simulations to better determine the exact communication flow and processes required for drone incidents. Updating of existing processes and operating procedures can keep rogue drone operators off guard and provide security forces opportunities for apprehension.

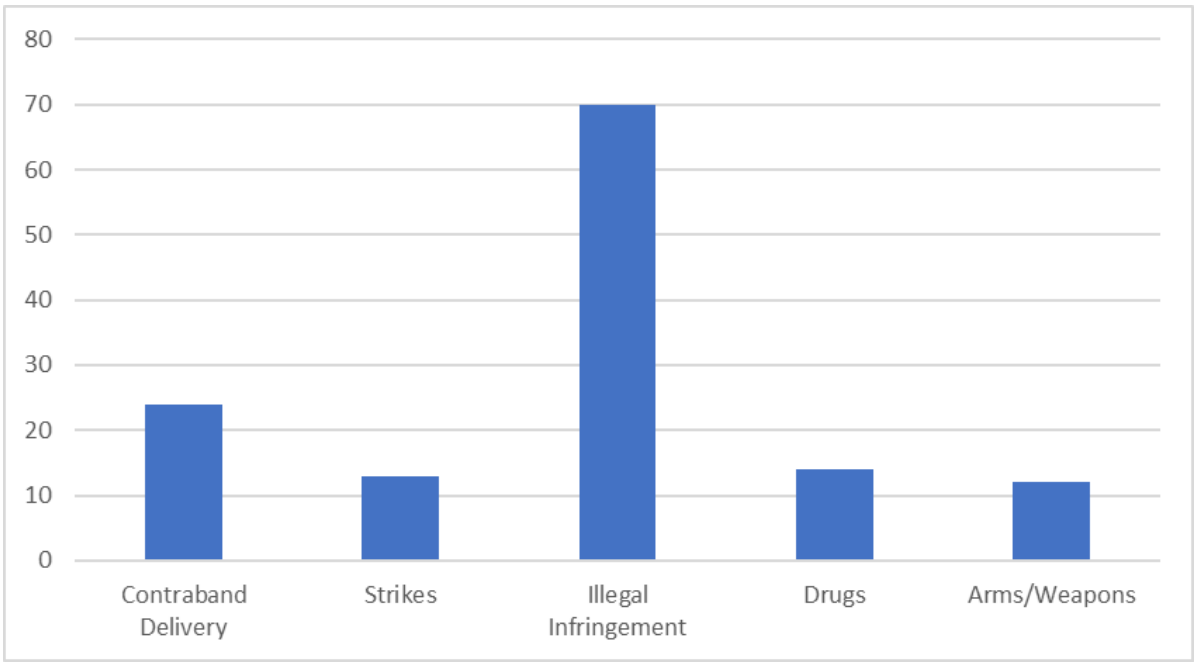


Figure 5: Number of Drones Incidents by Category of Activities (Since January 2020)

-

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:

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 originate from the USA, India and the UK. The 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.

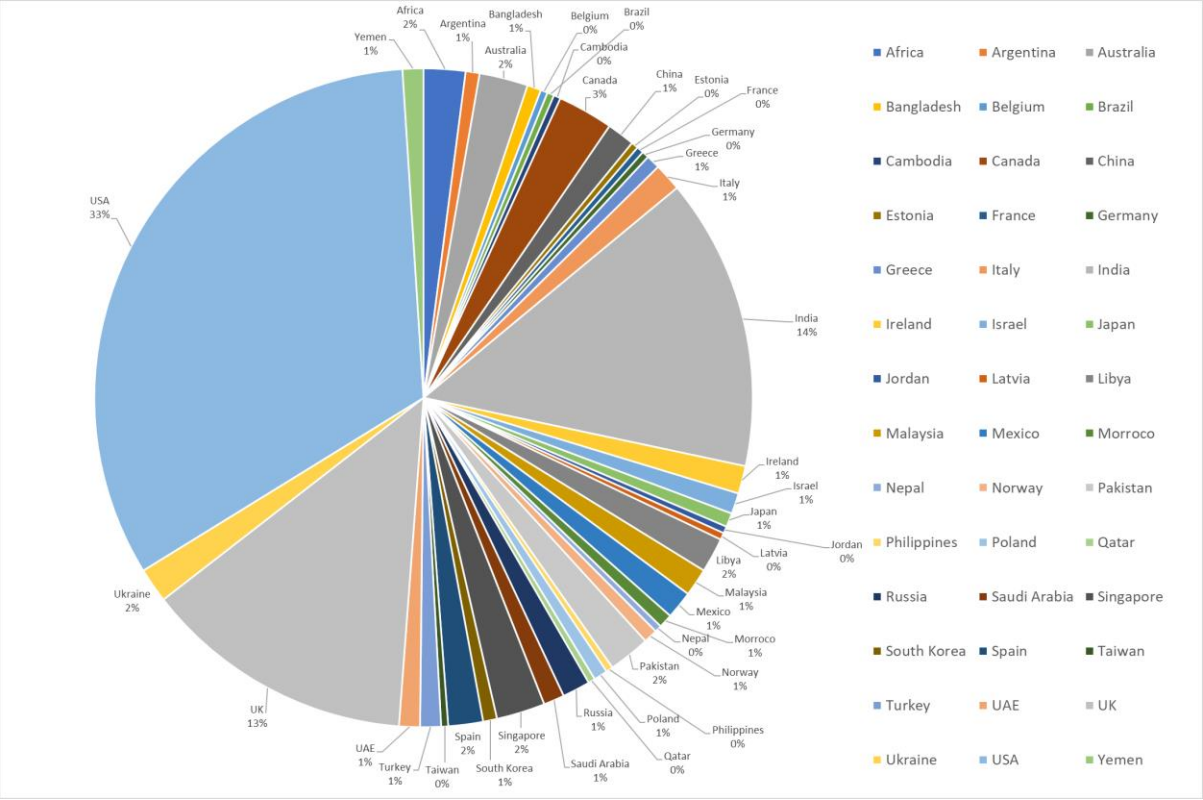


Figure 6: Percentage of Drone Artefacts by Country of Occurrence (Since January 2020)

-

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).

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.

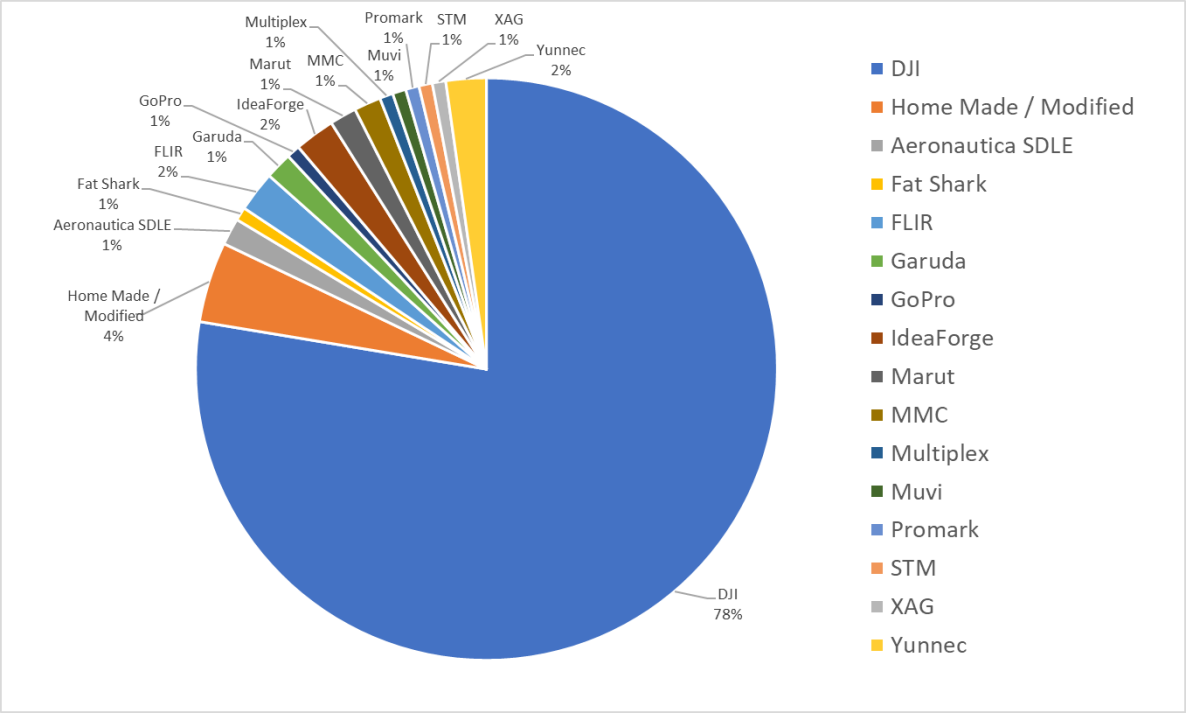


Figure 7: Percentage of Brands of Drones Utilised (Since January 2020) from our recorded artefacts. <1% is displayed as 1%.

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.

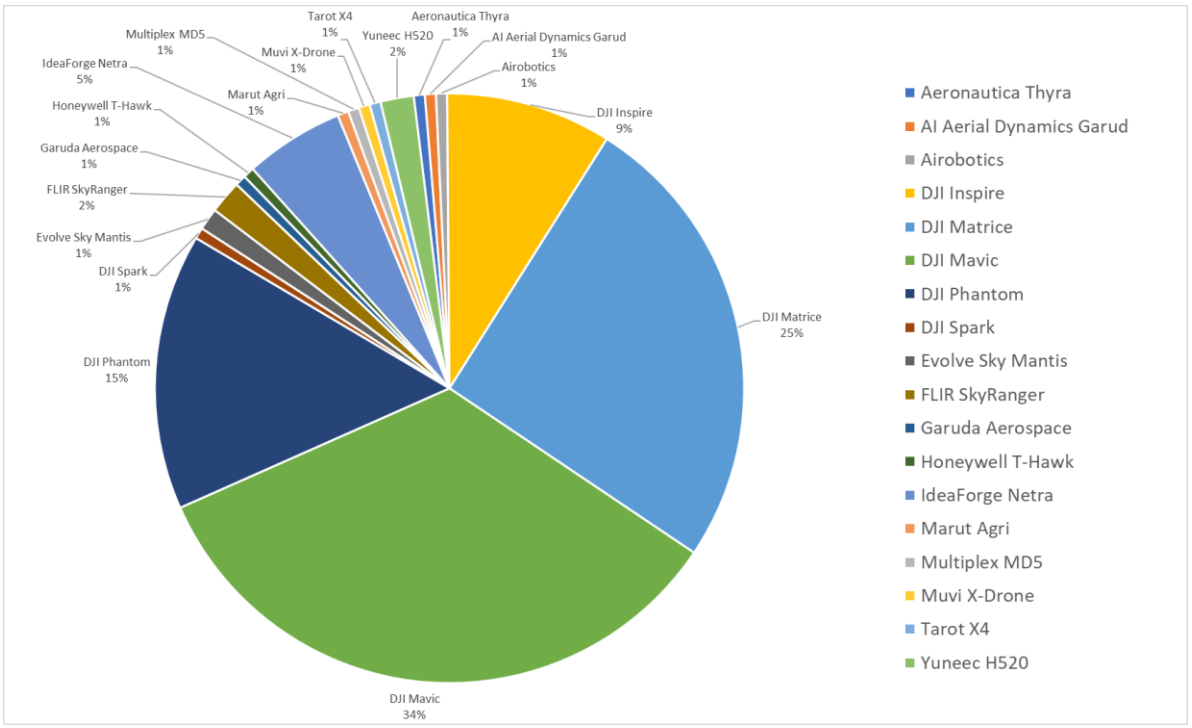


Figure 8: Percentage of Drone Utilised by Enforcement Agencies by Drone Model (Since January 2020)

That concludes our monthly roll up for the artefacts we have consolidated from January 2020 to June 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.

Notice to our readers: our featured advisories will slowly cease to be publicly available as DroneSec Notify moves to the online platform. Featured advisories have provided context and field-based learnings to important issues. However, with the ever-growing database that we have, DroneSec has moved onto an online repository where artefacts and reports can be tracked, classified and analysed much easier. Featured Analysis from now on are more comprehensive, wider in spectrum but only available on the Notify platform.

We thank you for your continued support thus far and we do look forward to having you together on our online Notify platform. Featured Advisories (only) will cease from 2nd July 2020; however, the free unclassified restricted PDF newsletter will still be available.

Intrusion and Trespass	Priority
Pakistan downs Indian DJI Mavic 2 for intruding 850m into Hot Spring Sector	**P2**

Summary

An Indian operated DJI Mavic 2 infringed 850m into Pakistan and was shot down by Pakistani border forces.

Overview

The Pakistan Army spotted a DJI Mavic 2 drone flying in Hot Spring Sector along the Pakistan-India Line of

Control (LOC). The drone was 850m into Pakistan when the Army shot it down. This drone marks the 9th drone that has infringed into Pakistan from India since 2020.

Analysis

This is a well-known occurrence between India and Pakistan where drones are sent continuously between both nations to spy and survey on each other. However, there are multiple incidents where drones used were also transporting weapons and contrabands to fund and fuel capabilities of terror groups such as Jaish-e-Mohammed, which saw one DJI Matrice, carrying a M4 rifle, shot down by the Indian Border Security Forces. India is looking for more and have installed counter drone systems at various points around the Indian side of the border along the LOC.

Small unmanned systems are like the DJI Mavic drones are an effective way of conducting surveillance. The drones are small and can be hard to spot with the naked eye. It gives offenders a good chance to avoid detection and capture by law enforcement agencies. In addition, the low price point and availability of such drones makes it an easily accessible tool.

Tracked Actor Category:

- India-Pakistan Border Drone Smugglers

Motivation and Goals:

- To conduct surveillance, reconnaissance, deliveries and possibly conduct acts of terror

Tactics, techniques and procedures:

- Use of unmanned systems to overcome difficult physical terrain and personnel control barriers
- Use of unmanned systems as a battlefield tactical advantage
- Use of unmanned systems to separate the distance and risk between operators and drone
- Sourcing cheap and available Commercial-Off-The-Shelf (COTS) drones for possible one-way flights
- Self-taught in unmanned and contraband-delivery UAS flights and operations
- Possibly self-taught in engineering and modifying of drone parameter and hardware components
- 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 and equipment types:

- Quadcopters, Multi-rotors, Fixed-Wing

Recorded contrabands:

- 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

Recommendation

The risk of being traced due to forensics analysis on the telemetry, flight data, video and photo footages is a risk inherent for rogue operators. These data could easily show where the drone was launched and possible provide visual images of the operator and its environment. 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 stored within. Event analysis from the drone data and video footages could assist in recognising patterns and trends providing possible modus operandi of the operator(s) and may aid in seizure on future attempts of incursions. Each of these incidents should be also be logged and categorised.

For huge areas such as border protection, it is understandable for counter-drone and drone detection systems to be not readily available. DroneSec recommends all law enforcement agencies to be ready for more of such threats by having basic preparation measures set in place to respond to such incidents. A drone threat management plan and Standard Operating Procedure (SOP) should be drafted, or modified, to govern the process, people and methodology in handling a drone threat. For example, agencies should start taking notice of aerial infringements as opposed to the traditional lookout at water or land-based incursions and border patrols should also try to adjust their patrol timings and routes as these time schedules could have already been recorded and logged by the multiple surveillances conducted by adversary states.

References

https://tribune.com.pk/story/2252275/pakistan-army-shoots-another-indian-spy-drone-along-loc

https://twitter.com/OfficialDGISPR/status/1277264300026015744

After July 2nd, 2020, featured advisories will be available to paid subscribers only. Contact info@dronesec.com to arrange a demo or visit https://dronesec.com/pages/notify to learn more.

Intrusion and Trespass	Priority
Criminal gangs in Nakuru, Kenya using drones to monitor security agencies during crimes	**P2**

Summary

Criminal gangs in Nakuru have recently been noted to use drones to monitor security agencies before carrying out crimes.

Overview

The Nakuru County Commissioner announced that he has received information that gangs in Nakuru have used drones to monitor activities and movement of security agencies before carrying out their crimes. Security agencies in Nakuru are taking this information seriously and have blamed politicians who were rumoured to be funding youths with drones, which sparked such illicit acts of drone surveillance by criminal gangs. These gangs used drones on the pretext of gathering news but instead, are monitoring law enforcement agencies while carrying out criminal activities.

Analysis

There are multiple criminal and youth gangs in Nakuru such as White Eagle and Confirm who are known to be violent and territorial. However, it is only recently that we have heard of these gangs using drones as part of

their tactics despite the fact that it is not easy for youths to purchase a drone, which are considered an expensive commodity in Kenya.

Compared to other incidents worldwide, we have seen drone used by cartels to perform multiple surveillance before the delivery of narcotics or other criminal activities. In the case of Nakuru, it is of no surprise that these surveillances will increase together with crime rate as these gangs grow more frustrated with joblessness within COVID-19.

Recommendation

Law enforcement agencies in Nakuru should be ready for a surge in drone surveillance by criminal gangs and DroneSec recommends these agencies to have basic preparation measures set in place to respond to such incidents. A drone management Standard Operating Procedure (SOP) or incident response plan should be drafted to govern the process, people and methodology in handling a drone, collecting evidence and responding to potential drone operators in a pre-determined radius. Agencies should start taking notice of aerial infringements and adjust their patrol timings and routes as these schedules could have already been recorded and logged by the multiple surveillance conducted by criminal gangs.

To go one step further, DroneSec recommends for the Nakuru security agencies to undertake mock simulations in reacting to such rogue drone incidents to test and hone their response, improve communication flow between participating agencies and practice on the logging and monitoring of drone cases. These simulations can aid law enforcement agencies in timing their response, mitigate risk and surface any challenges during the process.

References

https://www.nation.co.ke/kenya/counties/nakuru/nakuru-gangs-use-drones-to-fight-police-1253598

After July 2nd, 2020, featured advisories will be available to paid subscribers only. Contact info@dronesec.com to arrange a demo or visit https://dronesec.com/pages/notify to learn more.

1.4. NEWS AND EVENTS (P3)

NTSB finalises report on mid-air drone collision with manned helicopter

https://app.ntsb.gov/pdfgenerator/ReportGeneratorFile.ashx?EventID=20191205X95005&AKey=1&RType=Final&IType=IA&fbclid=IwAR0l00KYXjXzoyzQoQZoSeJXqir4xvJKmId4LzlpHNnAp-7VXBAsXBRFfaY

Multiple drone sighting complaints result in police broadcast, Wrexham, Wales UK

https://www.leaderlive.co.uk/news/18550362.police-call-consideration-persistent-use-drones-wrexham/

1.5. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P3)

ANSI releases version 2.0 standardisation roadmap for UAS

https://www.unmannedsystemstechnology.com/2020/06/version-2-0-of-ansi-uas-standardization-roadmap-published/

NASA publishes findings on technical capability of UTM operations in an urban environment

https://utm.arc.nasa.gov/docs/2020-Rios-Aviation2020-TCL4.pdf (PDF Document)

Increasing need for counter drone technology for Pakistan (commentary)

https://thegeopolitics.com/the-increasing-significance-of-anti-drone-technology-for-pakistan/

Understanding UTM and sharing of airspace data (commentary)

https://www.forbes.com/sites/forbestechcouncil/2020/06/05/where-utm-fails-to-fly/#1c6e58c868ef

Radio Frequency Jamming for C-UAV Applications (commentary)

https://ludbey.net/home/radio-frequency-jamming-for-c-uav-applications

A Quick Guide on Mobile Drone Detection (commentary)

https://aerodefense.tech/wp-content/uploads/IACP-Police-Chief-June-2020.pdf?utm_source=linkedin&utm_medium=social&utm_campaign=IACP%20magazine%20article

Unmanned Aerial Vehicle Routing Problems: A Literature Review

https://www.mdpi.com/2076-3417/10/13/4504/pdf (PDF Document)

1.6. COUNTER-DRONE SYSTEMS (P4)

US Army announces counter drone systems that meets its selection criteria

https://www.army.mil/article/236713/army_announces_selection_of_interim_c_suas_systems

IAI and Iron Drone to integrate kinetic drone interception capabilities into IAI's Drone Guard

https://www.iai.co.il/iai-and-iron-drone-collaboration

US Army looks into plug and play counter drone technologies for interoperability

https://www.army.mil/article/236839/army_picks_countermeasures_against_drones

Thailand awards contract to Ascent Vision Technologies for X-MADIS counter drone system

https://ascentvision.com/ascent-vision-technologies-secures-cuas-contract-with-key-thailand-defense-agency/

1.7. UTM SYSTEMS (P4)

Altitude Angel's GuardianUTM to be deployed at Cranfield Airfield for evaluation and test usage

https://www.altitudeangel.com/news/posts/2020/june/cranfield-airport-deploy-altitude-angel-guardianutm-platform/

Switch and ANRA Technologies to validate UTM technology for national scale deployment

https://www.anratechnologies.com/home/news/anra-technologies-to-commence-utm-tests-at-unprecedented-scale/

Altitude Angel and AIRVID partner for drone operations GuardianUTM platform solutions

https://www.altitudeangel.com/news/posts/2020/june/altitude-angel-airvid-global-partnership-programme/

1.8. INFORMATIONAL (P4)

Drone crash retrieval confronted by Vernon resident with firearm, Connecticut USA

https://patch.com/connecticut/vernon/drone-crashes-vernon-yard-gun-charge-follows

Turkish Armed Forces continue testing ALPAGU, a tactical strike kamikaze drone by STM-DT

https://www.dailysabah.com/business/defense/new-kamikaze-drone-alpagu-expected-to-join-turkish-security-forces-at-end-of-2020

Chinese military CH-92 drones arrive in Batajnica air base, for Serbian Air Force

http://rs.n1info.com/English/NEWS/a615186/Chinese-military-grade-drones-arrive-in-Serbia.html

Herkimer PD adds DJI Mavic Mini and DJI Mavic 2 as part of their operational assets, NY USA

https://www.uticaod.com/news/20200630/herkimer-pd-adds-drones-to-list-of-tools

Waterloo Regional Police track and locate man in distress with the help of drones, Canada

https://globalnews.ca/news/7111433/waterloo-police-drone-manitou-and-bleams/

DJI launch drone rescue map to visualise drone intervention within rescue operations

https://enterprise.dji.com/drone-rescue-map/

1.9. DRONE TECHNOLOGY (P5)

Parrot launches ANAFI USA drone with tough security and encryption measures

https://blog.parrot.com/2020/06/30/anafi-usa/

Ontario Fire and Rescue purchase DJI Flight Simulator for skills training on drone operations

https://www.argusobserver.com/news/ontario-fire-and-rescue-receives-grant-for-drone-simulation/article_ab4967ee-b8c4-11ea-8208-5b01ea1f1815.html

US Air Force releases concept video of networked manned-unmanned air warfare

https://www.thedrive.com/the-war-zone/34351/glitzy-air-force-video-lays-out-skyborg-artificial-intelligence-combat-drone-program

1.10. SOCIAL (P5)

Fortem Technologies hosts Countering Drone Threats webinar

https://www.youtube.com/watch?v=I7_h2pugXIA&feature=emb_logo

Wicklow Civil Defence Drone Unit utility and training on their DJI Matrice 200

https://twitter.com/wicklowcoco/status/1278206941655904257

Using MAVLink, ArduPilot to aggressively fly small UAS in small, complex environments

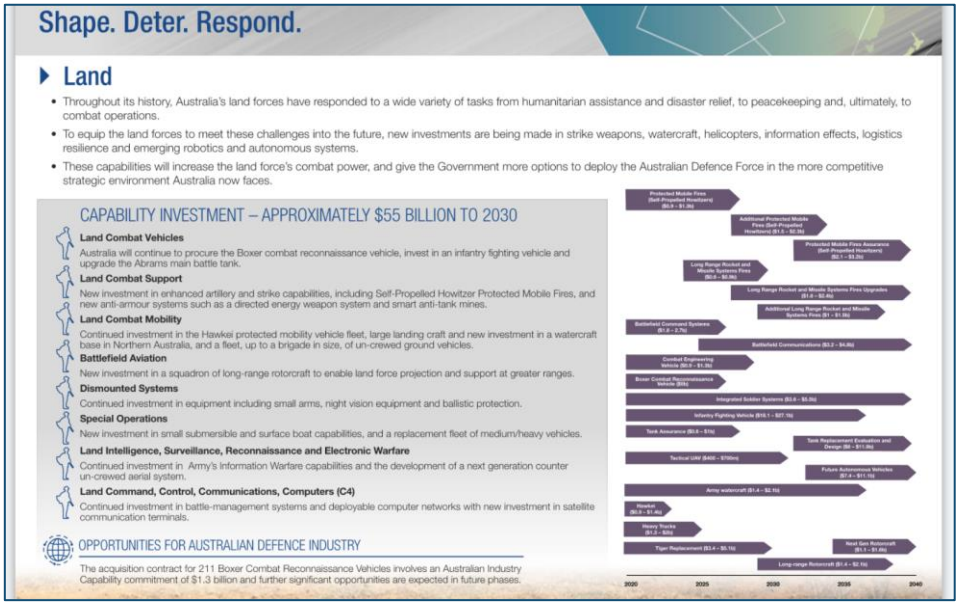
https://hackaday.com/2020/06/30/aggressive-indoor-flying-thanks-to-steamvr/

Drone Security for Critical Infrastructure (Video)

https://www.youtube.com/watch?v=u_qv1Sbnllg (Part 1)

https://www.youtube.com/watch?v=gfoiZtsFG78 (Part 2)

Australian DoD to invest in tactical UAS, counter un-crewed aerial systems up to 2030



Two Turkish drones downed at Deralok near Zhako, Iraq

https://twitter.com/dersi4m/status/1278240466757189632

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.

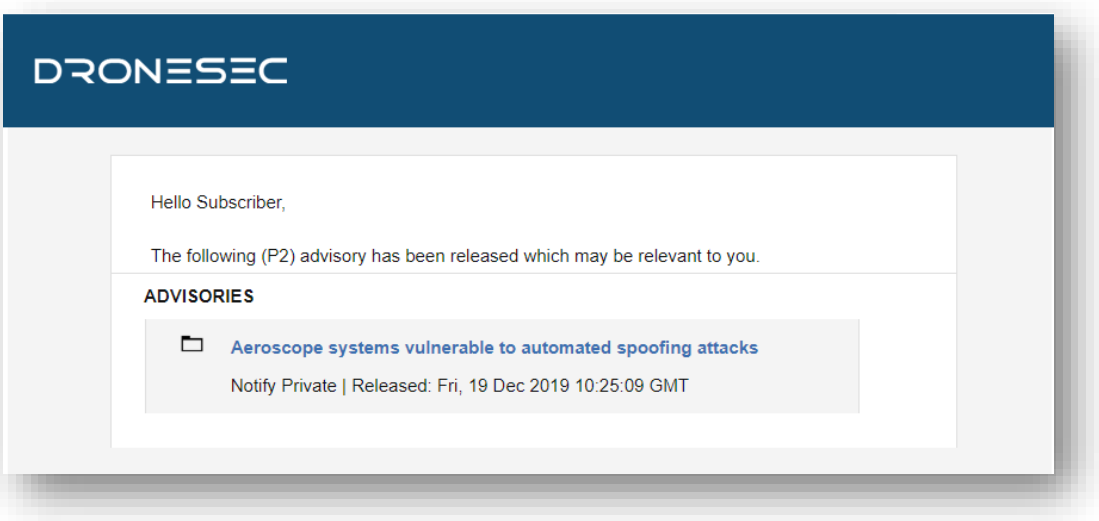


Figure 9 - A threat notification specific to a Notify customer's listed keywords.

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.