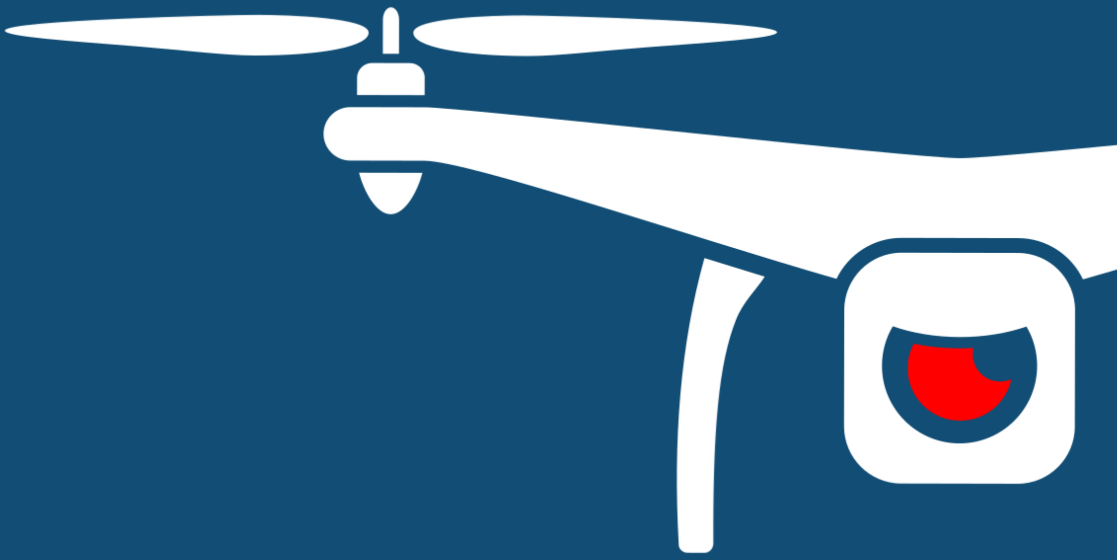
DRONE SEC
A Privasec COMPANY

NOTIFY ISSUE #34 (PUBLIC)

WEEKLY THREAT INTELLIGENCE

05 August 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**

The month of July has come and gone. For our Melbourne office, we are in Stage 4 COVID restrictions with an 8pm curfew to boot! End of the month signals our monthly roll-up, so we are taking a look back at some of the statistics and insights from the monthly artefacts.

Mid-July saw the release of URSA Inc's Counter-UAS Analytics Platform (CAP), which analyses telemetry data from UAS systems and sensors. A unique approach towards connecting and visualising CUAS data in a way that can help both investigators and vendors inform their future product development. Towards the end of July, we put out a Request for Information on behalf of URSA; this was targeted at UAS incidents and investigations within the energy sector. David Kovar and company are doing analysis in this sector and are seeking industry information or contributions – please get in touch with us or URSA Inc directly at info@ursasecure.com if you'd like to take part.

On a personal note, I make it no secret that DroneSec as a firm likes to model our operations off a combination of two highly regarded entities - Palantir and DIU's 'Rogue Squadron'. Our culture is unique, but we take motivation from the technologies and strategy employed by these firms in the way they tackle unique industry (and defence) challenges. It was great to hear from the founder of Rogue Squadron, Mark Jacobsen and many readers may find it interesting as well, given the mix of both government and private firms.

Another highlight this week is the cyber-security guidelines issued by India's aviation authority. Will other countries follow suit in implementing these controls? Will the measurement phase reveal challenges to innovation or speed up innovation with safer, more secure operations? Time will tell, but we'll be closely watching this one. As we speak, DroneSec is actively trying to bring the successful CREST ASSURE scheme/accreditation (as under the UK CAA) within the APAC region; potentially something that might allow a quicker sync time if similar cyber-specific guidelines (to India) were to be implemented here. For bed-time reading, I highly recommend 'Camouflage SOP: A guide to reduce physical signature under UAS'. All this and more in this week's brief, below.

Reminder: Our Global Drone Security Network is virtual and scheduled for September 18th, 2020.

We have various speakers from the CUAS, Law Enforcement, Security Surveillance and Threat Intelligence sectors providing insights into unmanned security-specific topics. We also have several interesting reports, white papers and tooling expected to be released during the event specific to the industry.

As we are in the final stages of confirming our speakers, please send your talk Topic, Description and Bio to info@dronesec.com if you would like to be considered to take part. The event will be free and following its inaugural event in Singapore, is the only of its kind focusing specifically on drone security, counter-drone and cyber-UAV topics.

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.

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

July in Summary

In 2020 thus far, one thousand, two hundred and eighty-eight artefacts were recorded which roughly equates to about 6 drone security 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.

A caveat from the Threat Intel team: with the inclusion of our Notify Threat Intel Platform, it's easier and more automated to collect incidents and events. Even though this is a factor, the increase of artefacts has remained quite steady over time (platform launch was on 23rd June).

Month	Number of Artefacts	Global number of artefacts 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	7.3	19 (8.68%)
July	224	7.2	5 (2.32%)
Total (2020)	**1288**	**6.05**	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 July 2020: Notify release #4 – #33.

We see a 30% increase in artefacts on UTM Systems and a 25% increase in whitepapers and publications in the month of July 2020. Several collaborations were made between drone industry leaders on UTM development in the UK. UTM Systems are getting a lot of publicity nowadays due to widespread use of drones during COVID-19. Industries are seeing possible use of drones for Urban Air Mobility (UAM) or for Advanced Air Mobility (AAM), a term coined by NASA on the use of thousands of low flying drones in urban environment. This has in turn pushed for a number of publications on drone safety, security and the future state of air warfare for the military. We have also seen government granting special permits for the trials of autonomous air passenger vehicle, with the most recent one award to EHang.

Category	Number of Artefacts (**Jan – Jul 2020**)	Compared to Number of Artefacts (Jan - Jun 2020)
Featured	74	61
Cyber and Information Security	24	21
News and Events	266	240
Whitepapers and Publications	218	163
Counter-Drone Systems	106	86
UTM Systems	68	47
Drone Technology	132	105

Incident Summary

DroneSec recorded multiple cases of drone utility and innovation rising globally such as anti-jamming flight modules and bird-like drones that can move and evade like a hummingbird. 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.

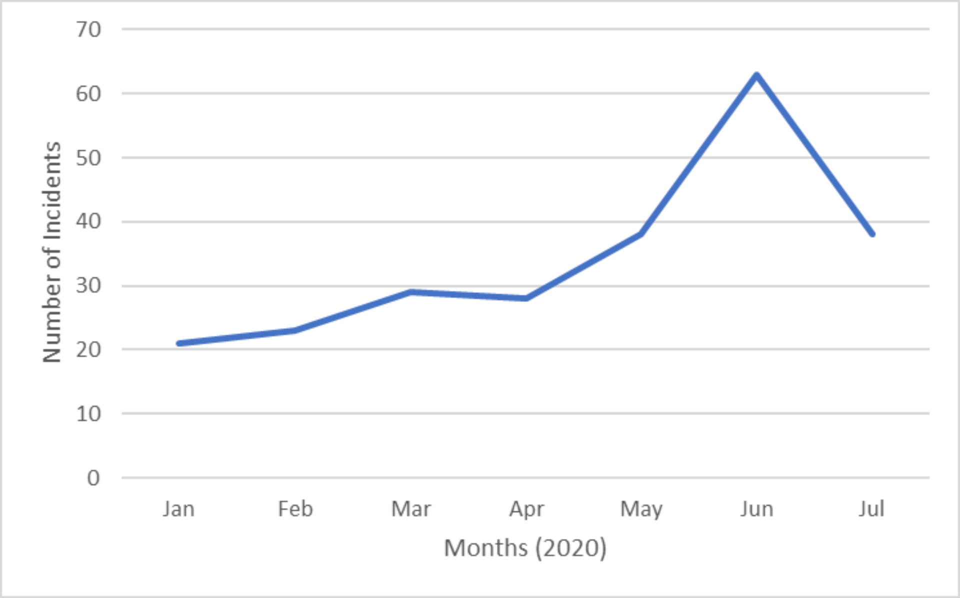


Figure 1: Number of Drone Incidents for the Year 2020

The number of drone incidents took a dip in the month of July 2020, however, that cannot be inferred as a safer drone operating environment. There are still close to 40 cases of drone incidents logged and a majority of the incidents were committed due to trespass and intrusions into restricted areas. DroneSec recorded more than a 20% increment in number of drone incursions into event locations and international airports. Although it was not known if the act was committed due to negligence of aviation laws, such acts are a hazard to the lives of aviators and civilians.

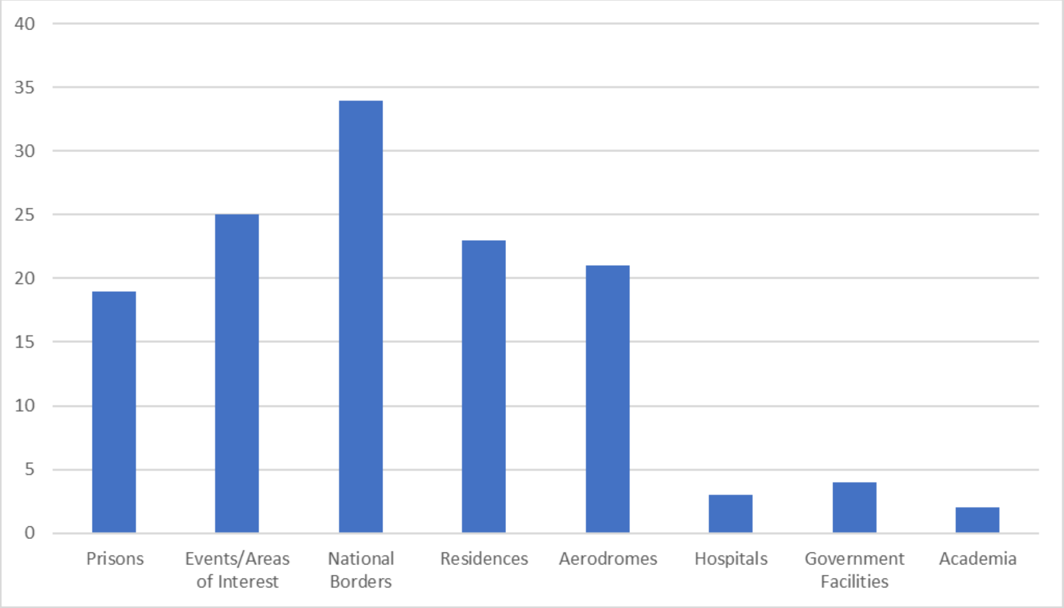


Figure 2: Number of Drone Incidents by Location of Occurrence (since January 2020)

From all the drone incidents that were recorded, DroneSec observed that only 54% of drones sighted (during incidents) were seized by law enforcement agencies, either by firing at them (with traditional calibre ammunition guns) or in haste to escape, the drones had crashed or gotten stuck in trees. Of the remaining 46%, these drones not found despite a thorough search in the vicinity. 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 despite engaging external security practitioners. DroneSec has always recommended for a drone management plan; without one, rogue drone operators will only continue to be more brazen with each successful attempt.

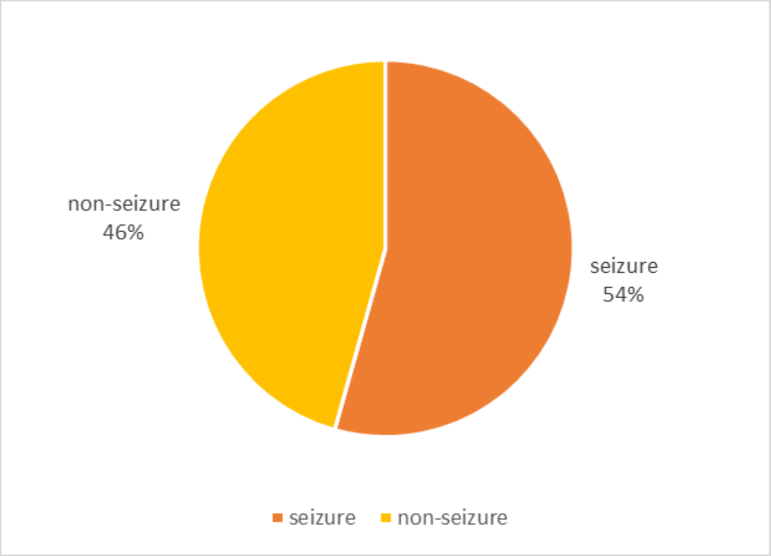


Figure 3: Percentage of drone incidents where the drone system was seized

Conversely, only 24% 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.

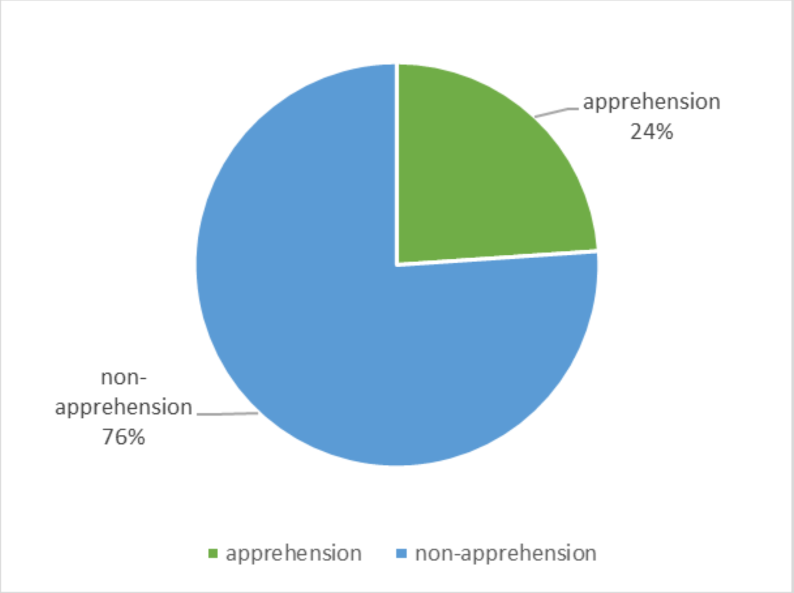


Figure 4: Percentage of drone incidents where the drone operator was apprehended

The stark difference in percentage on the seizures of drones against the apprehension of the drone operators goes to show that existing counter drone systems may only be geared towards capturing or downing of rogue drones. The gap in arresting the operator responsible continues to exist, which should be addressed, otherwise, drone intrusions will only continue to increase as the use of drone grows exponentially.

DroneSec Recommendations

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 $7,500 - $4,000,000 against a $400 - $80,000 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 there is no one-size-fit-all counter drone solution managed by a core central team, a better approach would be to have a layered defence, starting with education and training for personnel. Having a drone management plan and forensics/incident response plan will serve as a good starting base for most agencies facing drone threats. Counter drone systems will aid to complement these training and improve on drone mitigation strategies.

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

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: Featured advisories have provided context and field-based learnings to important incidents within the drone ecosystem. 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 or to paid subscribers. If you would like continued featured summaries such as the example, please get in touch with us or purchase a subscription.

Cyber-UAV Security	Priority
Synacktiv release follow-up DJI report regarding Android commercial app security analysis	**P2**

Summary

In a follow-up report to their initial analysis of the DJI GO4 application, security firm Synacktiv have released a report regarding the commercial Android app – DJI Pilot.

Overview

The report explains that the firm detected similar security issues detected in the initial GO app, including the forced update mechanism. DJI has responded to the second report, stating that:

"We are dismayed that safety features have again been misunderstood and misconstrued as hypothetical security threats by researchers who are evidently unfamiliar with the operation being the other of drone technology."

Analysis

This artefact has just been released and as a result, is still being analysed by the DroneSec team. Meanwhile, some chatter has been observed around writer Scott Simmie at DroneDJ who questions the credibility of the reports aligned with the launch time of the Parrot Anafi USA; however, the article does not analyse the secondary findings report by security firm Grimm.

Our continued approach to these situations is for any organisations using drones to do their own or independent analysis if questioning 3rd party reports or manufacturer's security whitepapers. As demonstrated in the previous Synacktiv release, DJI did make some changes to their GO4 app based on the recommendations provided, but historical app versions allow any researcher to verify findings with their own analysis.

References

- Updated DJI Pilot App Report: https://www.synacktiv.com/en/publications/dji-pilot-android-application-security-analysis.html
- DJI Vendor Response: https://www.dji.com/newsroom/news/dji-statement-on-further-misleading-claims-about-app-security
- DroneDJ query on credibility of Synacktiv report: https://dronedj.com/2020/08/04/another-allegation-that-djis-software-has-security-issues/

Intrusion and Trespass	Priority
Drone operator apprehended for flying drone over restricted airspace of F1 track in Silverstone	**P2**

[redacted]

Security	Priority
India’s Bureau of Civil Aviation Security lists out security guidelines for drone operating systems	**P2**

Summary

India's aviation security regulator listed out rules to govern the security of drone storage facilities and drone operating systems and piloting systems.

Overview

India's aviation security regulator, Bureau of Civil Aviation Security (BCAS), recently listed out rules for operating systems and piloting systems for drones. A remote piloting station was defined by the Indian authority as a system which has command and control capabilities and any other components that aid in the operation of drones. These systems are deemed as similar in purpose and design to a manned aircraft's cockpit, however, have the additional vulnerability of being exposed to external threats, sabotage and interference.

BCAS introduced the need to ensure that cyber and physical security of the system is well maintained and must be managed in a way that tampering is prevented, and integrity is upheld. Measures such as regulated access control, background checks and training for involved staff, installation of CCTV cameras and 30 days storage requirement for all audio-visual footage are included in the regulation. These measures were to ensure that the safety and security of data, communication links and services of drone operations.

BCAS also included that all drone operators and organisations were required to implement and maintain a security programme for drones above and beyond the necessary permissions and permits required for certain drone operations.

Analysis

This is an important step in maintaining a secure drone operating system from possible intrusion, hijacks and sabotage plays a critical role in drone operations. Drone piloting systems are very similar to the ground control stations that are used in the command control of military drones. It controls not only the flight profile of drone, but also its sensor and payload capabilities - including missiles and bombs for combat-enabled UAVs, or also known as UCAVs.

A number of critical IT systems not only have guidelines (e.g. NIST, MITRE, ASD Essential 8) but legal requirements to be security tested by an independent assurance organisation. Increasingly, drone systems are interconnected (UTMs) and have multiple technology stacks supporting their operations. Cyber-specific vulnerabilities exist throughout the systems, applications and infrastructure and should be incorporated within the design, development and operations of commercial drone programs.

It's likely that we'll see accreditations, standardised methodologies and certifications in the very near future that cover this angle of Cyber-UAV security assessments within the drone ecosystem.

Recommendation

DroneSec recommends other civil aviation authorities adopt a similar form of guidelines as India, to secure the operating and piloting systems for drones. In addition, training of security personnel, operators and any workers that could be affected (both directly and indirectly) by drones is essential too. This training will aid to hone responses and improve communication flow during incidents and allow all participating agencies to respond effectively during time critical scenarios and mitigate possible risks from drone threats. These types of initiatives need to come from the top, involve industry peers and contribute to the wider knowledge base of drone security.

References

https://timesofindia.indiatimes.com/india/bcas-issues-security-guidelines-for-drone-operating-systems/articleshow/77313844.cms

https://www.newindianexpress.com/nation/2020/aug/02/aviation-security-regulator-issues-security-guidelines-for-drone-operating-systems-2178110.html

Intrusion and Trespass	Priority
ISIS sympathiser remodels drone with weapons for possible attack	**P2**

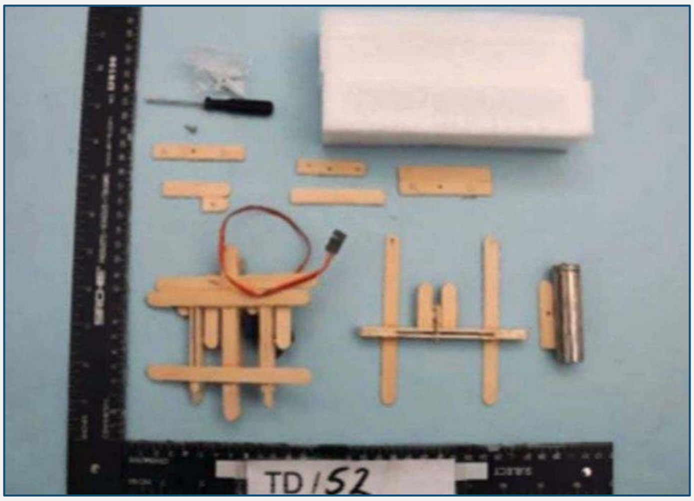
Summary

An ISIS supporter was reported to the police by his landlord after a discovery of weapons stored within his rented unit.

Overview

Hisham Muhammad, an ISIS supporter, was planning on carrying out attacks in London, but was detained when his landlord reported to the police his discovery of weapons such as knives, tomahawk, machete and axes within the unit. The police discovered that Muhammad had been planning for an attack and was researching on release mechanisms for commercial drones which allowed him to carry out aerial terror attacks.

Masks, camouflage clothing, stabbing cardboard boxes and drawings of bladed weapons were also found within his place of residency. Muhammad's cousin, Faisal Abu Ahmad, was also arrested for not alerting authorities of the attack plan despite knowing of Muhammad's intentions.



Recorded Threat Actor: *Islamic State of Iraq and Syria (IS/ISIS/ISIL)*

Recorded Member Groups:

- Islamic State of Iraq and the Levant (ISIL)
- Islamic State (IS)
- Mohamed Yassin Amrani (Arrested)

Motivation and Goals:

- To conduct acts of terror via a drone with explosive payloads attached

Tactics, Techniques and Procedures:

- Use of unmanned systems to conduct surveillance, reconnaissance and destructive combat missions
- Use of unmanned systems to cause terror or causalities in urban and civilian environments
- Use of unmanned systems to effect explosives without the use of a suicide sacrifice
- To extend the range of terror while ensuring a separation between the operators and weaponised payloads
- Sourcing cheap and available Commercial-Off-The-Shelf drones for actions aligned with terrorism
- Sourcing cheap modifiable drones off the black market or second hand market
- Extending the range and payload-carrying capacity of COTS drones for malicious missions by modding
- Training war fighters and soldiers in unmanned and counter-drone UAS flights and operations
- Using small COTS drones to drop explosive payloads (mortars, grenades ~<1 kg) on civilians or military units, often with shuttlecocks or home-made flight guidance mechanisms
- Using custom and purchased amplifiers, transmitters, receivers, antennas, extenders and dual-battery components to improve the overall range and targeting of limitations by OEM systems

Recorded Use of Drone/Equipment:

Quadcopters, Multi-rotors, VTOL UAV, Fixed-Wing

Recorded Contraband/Crime:

Drones attached with explosives/modified grenade

Recorded Area of Operations:

- Syria
- Baghdad, Iraq
- Barcelona, Spain

Reports / Artefacts Recorded:

Arrest of ISIS member reveals attack plan to bomb Camp Nou Stadium with drone (19 May 2020)
https://notify.dronesec.com/reports/5887bc30-a090

Iraqi Joint Operations Command takes down four ISIS suicide bombers with combat drone (12 Jul 2020)
https://menafn.com/1100472104/5-IS-suicide-bombers-2-security-members-killed-near-Baghdad

Analysis

The use of explosive-laden drones by IS/ISIS/ISIL has transitioned from battlefield tactics to use within urban and civilian environments. With the rise in use cases of drones globally, more people, and malicious actors, are seeing the benefits of drones. Although not common within ISIS, this incident reflects the growing use of drones to carry out illicit operations and attacks. Organised crime groups and lone wolf terrorists are realising that drones are an innovative solution to complement traditional methods of war crimes.

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. Offenders for such acts tend to get away easily as many common public areas do not yet possess drone detection or counter-drone systems to mitigate the threat.

Operating the drone itself has a low skill barrier, however, in this situation, some operator experience and domain knowledge required in developing the release mechanism and remodelling of the drone. Based on the photo, it does seem like the remodelling design phase was in its rough stages with 'ice cream sticks' used to construct the basic structure of the drone. These are good information that the English law enforcement have managed to collect – it is important this documentation is properly analysed and assessed for informing future SOPs and modus operandi of ISIS.

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.

References

https://www.arabnews.com/node/1711751/world

Intrusion and Trespass	Priority
Police investigate sighting of drone flying near Frackville prison in Pennsylvania, USA	**P2**

[redacted]

Intrusion and Trespass	Priority
Low flying DJI Mavic 2 intrudes and halts baseball game in Minneapolis	**P2**

[redacted]

1.4. NEWS AND EVENTS (P3)

Azerbaijan military shoots down Armenian reconnaissance drone near Tovuz, Azerbaijan

https://www.aa.com.tr/en/asia-pacific/azerbaijan-downs-armenian-drone/1926676

Houthi claims shooting down RQ-20 drone in Harad, Yemen

https://www.aa.com.tr/en/middle-east/yemen-houthis-claim-downing-drone-near-saudi-border/1929756

Pakistani drone spotted near Hiranagar, India, search operation activated to find drone

https://zeenews.india.com/india/pakistani-spy-drone-spotted-in-jammu-and-kashmirs-hiranagar-sector-search-operation-launched-2299923.html

1.5. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P3)

EASA releases FAQ on drone regulations

https://www.easa.europa.eu/the-agency/faqs/drones-uas

Macao bans drone flights during government-sponsored helicopter tourism rides

https://macaunews.mo/drone-flights-banned-during-chopper-tours/

Government officials favour more education to prevent drone intrusion during emergencies

https://www.graydc.com/2020/07/29/officials-support-more-education-to-prevent-illegal-drone-flights-over-wildfires/

The night a mysterious drone swarm descended on Palo Verde nuclear power plant (commentary)

https://www.thedrive.com/the-war-zone/34800/the-night-a-drone-swarm-descended-on-palo-verde-nuclear-power-plant

Drone Sightings: The Actual Non-Hyped Numbers Analysed (commentary)

https://www.suasnews.com/2020/08/drone-sightings-the-actual-non-hyped-numbers-analyzed/

Middle East offers Singapore some lessons on countering rogue drones (commentary)

https://www.todayonline.com/commentary/middle-east-offers-singapore-some-lessons-countering-rogue-drones

How to hide from a drone – the subtle art of 'ghosting' in the age of surveillance (commentary)

https://theconversation.com/how-to-hide-from-a-drone-the-subtle-art-of-ghosting-in-the-age-of-surveillance-143078

Education will be key to curb misuse and drone incidents in Malaysia (commentary)

https://www.thestar.com.my/metro/metro-news/2020/08/04/education-key-to-proper-drone-use-says-don

How drones affect your threat model (commentary)

https://www.csoonline.com/article/3568452/how-drones-affect-your-threat-model.html

CIA Reveals Details of Bird-Like 1970s Stealth Drone — With Planned Nuclear Propulsion (commentary)

https://www.forbes.com/sites/davidhambling/2020/07/31/cia-reveals-details-of-bird-like-1970s-stealth-drone---with-planned-nuclear-propulsion/#5ba2d3ef428e

What are the damages on a plane when it collides with a small plane (test)? (commentary)

https://dronedj.com/2020/08/03/drone-collisions-can-damage-manned-aircraft/

DroneDJ queries on credibility and source of DJI security assessments (commentary)

https://dronedj.com/2020/08/04/another-allegation-that-djis-software-has-security-issues/

Camouflage SOP: A Guide to Reduce Physical Signature under UAS

http://www.2ndbn5thmar.com/camouflage/SIGMAN%20Camouflage%20SOP%20200630.pdf (PDF document)

The Mental Health Risks Associated with Remotely Piloted Aircraft Operations

http://www.journal.forces.gc.ca/Vol20/No3/PDF/CMJ203Ep46.pdf (PDF document)

1.6. COUNTER-DRONE SYSTEMS (P4)

Numerica's MIMIR enables layered CUAS capabilities with sensor fusion and target tracking

https://www.numerica.us/numericas-mimir-advances-c-uas-capabilities/

India permits training of eagles in Telangana as part of counter drone measures

https://www.thehindu.com/news/national/telangana/eagle-squad-to-neutralise-drones/article32243252.ece

New York PD will deploy counter drone teams to deter drone intrusions during U.S. Open

https://www.tmz.com/2020/07/30/us-open-drones-nypd-covid-19-tournament-tennis/

SKYLOCK's anti-drone wearable armour has inbuilt drone detector and anti-drone jammer

https://www.calcalistech.com/ctech/articles/0,7340,L-3843211,00.html

1.7. UTM SYSTEMS (P4)

UK selects AiRXOS, Altitude Angel, ANRA Technologies, Collins Aerospace and Wing for Open-Access UTM framework

https://cp.catapult.org.uk/2020/07/30/open-access-utm-framework-launched/

Ehang receives Special Flight Operations Certificate for passenger drone flights in Canada

https://www.ehang.com/news/665.html

NASA Chief shares vision for UAM and advanced air mobility (commentary)

https://www.ainonline.com/aviation-news/general-aviation/2020-07-27/nasa-chief-uncrewed-aircraft-safer

1.8. INFORMATIONAL (P4)

Iran reveals Shahed 181 and 191 stealth UAV, reversed engineered from captured US RQ-170

https://theaviationist.com/2020/08/02/iran-showcases-shahed-181-and-191-drones-during-great-prophet-14-exercise/

Data shows more than 2,000 drone flights made by UK law enforcement for operations

https://www.coventrytelegraph.net/news/coventry-news/revealed-how-2000-police-drone-18683116

Hamden Police Department gets approval to purchase DJI Matrice 300 drone for operational needs

https://www.newhavenindependent.org/index.php/archives/entry/hamden_pd_buys_a_drone/

Drones to be deployed over Bear Creek Greenway, USA, to help prevent spreading wildfires

https://kobi5.com/news/drone-flights-to-begin-over-bear-creek-greenway-133560/

Bulzi chooses Draganfly for US DoD base security development project

https://www.globenewswire.com/news-release/2020/07/28/2068739/0/en/Bulzi-Selects-Draganfly-to-be-its-Sole-Provider-of-Drones-and-Aerial-Sensors-for-DoD-Base-Security-Development-Projects.html

Soarizon and Consortiq collaborate to promote safe and compliant drone operations

https://www.soarizon.io/news/soarizon-by-thales-and-consortiq-join-forces-to-offer-services-to-enterprises-using-drones

India deploys drone to surveil VIP routes during ceremony in Ayodhya

https://www.indiablooms.com/news-details/N/63673/ayodhya-wrapped-in-tight-security-cover-drones-used-to-vigil-vip-routes-for-ram-temple-groundbreaking-ceremony.html

Drone team activated to look for missing bodies near rapids along Bate Island, Canada

https://www.cbc.ca/news/canada/ottawa/police-missing-swimmers-bate-island-1.5671694

Switzerland secures Lockheed Martin's Indago 3 surveillance drone for military usage

https://www.janes.com/defence-news/news-detail/lockheed-martin-sells-indago-3-uav-to-switzerland

1.9. DRONE TECHNOLOGY (P5)

EHang launches 216F, a firefighting drone for high-rise buildings

https://www.ehang.com/news/670.html

StoreDot demonstrates 5 minutes ultra-fast charging for commercial drones

https://www.store-dot.com/post/world-s-first-5-minute-charge-of-a-commercial-drone

Ninox SpearUAV launched from a 40mm grenade launcher, will aid soldiers in tactical battles

https://www.janes.com/defence-news/news-detail/new-dimension-spearuav-unveils-capsuled-ninox-uas

Korean Air to provide hybrid-powered drones to Korea's military for testing

https://www.janes.com/defence-news/news-detail/kal-readies-hybrid-powered-uavs-for-south-korean-military

UK's Royal Navy showcases use of drones to support future naval operations

https://www.defenceconnect.com.au/key-enablers/6569-royal-navy-demonstrates-uas-technology-to-support-future-operations

Logos Technologies to deliver wide area motion imagery sensors for drones in the US Navy

https://www.c4isrnet.com/unmanned/2020/08/03/with-this-new-sensor-blackjack-drones-can-monitor-an-entire-city-at-once/

1.10. SOCIAL (P5)

Video footage of Armenia's suicide drone

https://www.youtube.com/watch?v=b7sH8ZUGqRY&feature=emb_logo

Interview with Mark Jacobsen, Defense Innovation Unit – Rogue Squadron (podcast)

https://markdjacobsen.com/2020/08/04/diu-ex-podcast-going-rogue/

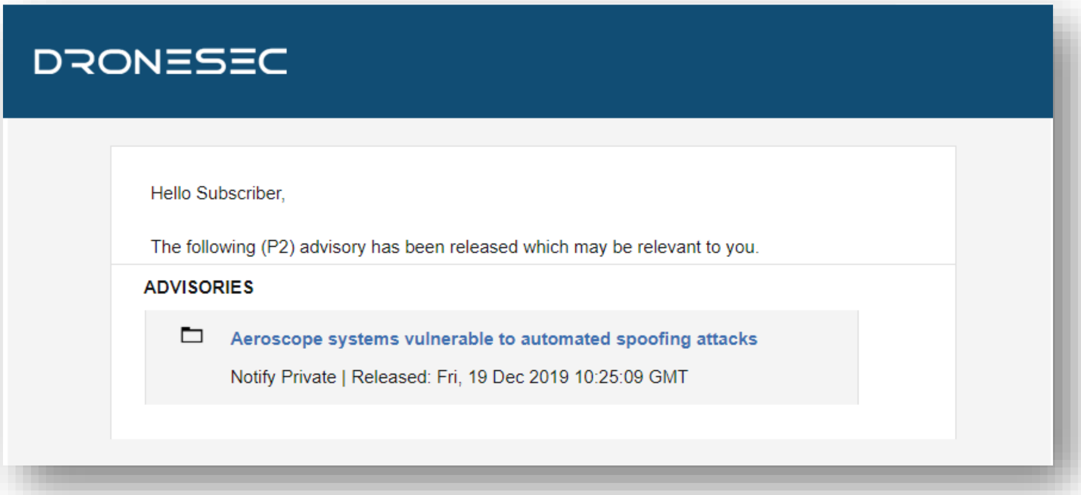
APPENDIX A: THREAT NOTIFICATION MATRIX

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.



DRONESEC

Hello Subscriber,

The following (P2) advisory has been released which may be relevant to you.

ADVISORIES

Aeroscope systems vulnerable to automated spoofing attacks

Notify Private | Released: Fri, 19 Dec 2019 10:25:09 GMT

Figure 5 - 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.