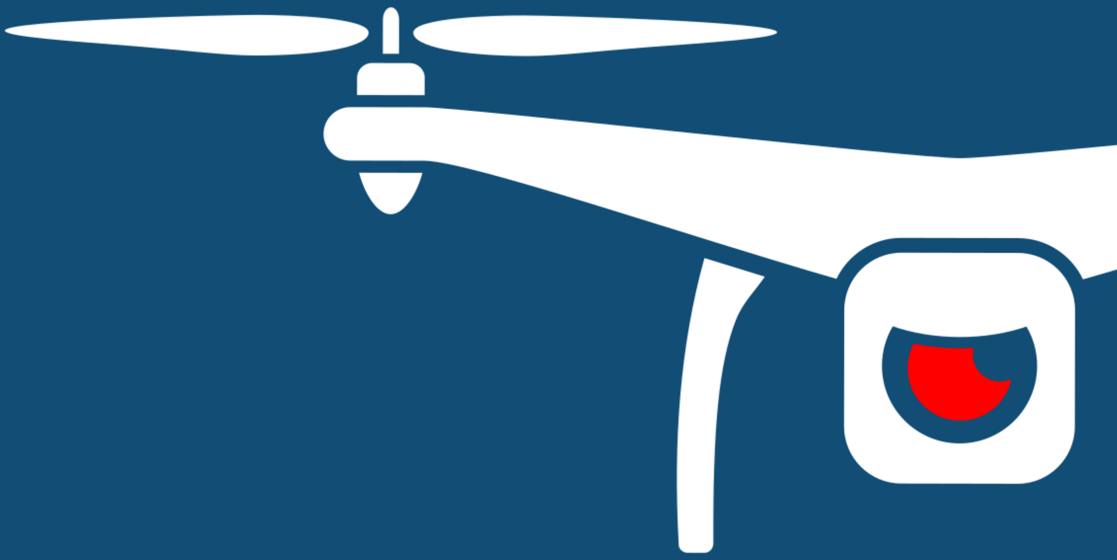
DRONE SEC
A Privasec COMPANY

NOTIFY ISSUE #47 (PUBLIC)
WEEKLY THREAT INTELLIGENCE

04 November 2020 | v1.0 RELEASE



UAS HACKING, HARDENING AND DEFENCE

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

DOCUMENT CONTROL

PREPARATION

DroneSec (dronesec.com)

Threat Intelligence Team

Email: info@dronesec.com

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

EXECUTIVE SUMMARY

Welcome to a new month and with that, a review of the past month October in drone incidents. Sometimes our analysts observe some interesting results, and October was no different. We saw quite a substantial increase in drone incidents and incursions in almost every industry except health. For some countries, this may be due to the relaxing of restrictions and the opening up of lockdowns.

Just last week we discussed how the FAA were being asked to look at a process for restricting airspace over critical infrastructure in the USA. This week, the Nuclear Regulatory Commission has published a very interesting memo after coordinating a technical analysis with Sandia National Laboratory to gauge the threat drones pose to plants. In conclusion, the report states that there are no risk-significant vulnerabilities that could be exploited by adversaries utilising commercially available drones. However, it is important to note they state from an adversarial perspective, this is due to the NRC's design-basis threat model (similar to a zero-trust model) which assumes adversaries already have insider information about a plant and its operations. It is understandable that Nuclear Power Plants are designed with threat modelling in mind – however, not all critical infrastructure undergoes this type of rigorous planning nor contains the same controls or security budget. It will be very interesting to see if this has any effect on the FAA's requests or if the space above power plants will remain open to drones (and superman-drone activists alike).

The DroneSec team have advocated the use of drone security and counter-drone frameworks since 2016, so it's always humbling to see it materialise around the world. In Australia, submissions closed for the Department of Infrastructure's Regulation Policy Paper including a Drone Security Framework. In the UK, the National Counter Terrorism Security Office released a simple and down-to-earth guidance piece on countering drone threats. On the other side of the pond, the Pentagon prepares to form a counter drone academy in Fort Sill, Oklahoma, in an effort to baseline doctrine, UAV Threat Actor TTPs (Tactics, Techniques and Procedures), methodologies and training. We're excited to play a part in these emerging efforts and surprised at the rate of adoption in which 2020 has shown so far.

So, what are the team reading this month? Hot off the press, the team grabbed the upcoming copy *"Countermeasures for Aerial Drones"* by Garik Markarian and Andrew Staniforth. All of the aforementioned articles, links and stories are below.

As always, if you have comments or feedback, want to join in the discussion in our slack group, or find out how we capture all this information please don't hesitate to contact us.

- *Mike Monnik, DroneSec CTO*

TABLE OF CONTENTS

1. Threat Intelligence ---------- 5
1.1. Introduction ---------- 5
1.2. Monthly Roll-up ---------- 6
1.3. Featured Advisories ---------- 12
1.4. News and Events (P3) ---------- 16
1.5. Whitepapers, Publications & Regulations (P3) ---------- 17
1.6. Counter-Drone Systems (P4) ---------- 17
1.7. UTM Systems (P4) ---------- 18
1.8. Informational (P4) ---------- 18
1.9. Drone Technology (P5) ---------- 18
1.10. Socials (P5) ---------- 19
APPENDIX A: Threat Notification Matrix ---------- 20
A.1. Objectives ---------- 20
APPENDIX B: Sources & Limitations ---------- 24
B.1. Intelligence Sources ---------- 24
B.2. Limitations ---------- 25

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 November, 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.

October in Summary

In 2020 thus far, one thousand, nine hundred and fifteen (1,915) artefacts were recorded which roughly equates to about 6 drone security artefacts per day**.** The number of events logged has an upward trend in the year 2020 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. Drone technology is growing at an exponential rate with new cutting-edge development seen weekly. This growth has also fuelled new methods of utilising drones; more sectors of industries are looking forward to capitalising on the advantages of drone and reduce overhead cost.

A caveat from the Threat Intel team: with the inclusion of our Notify Threat Intel Platform in mid-2020, it is 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.

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%)
August	206	6.6	-18 (-8.74%)
September	168	5.6	-38 (-22.62%)
October	253	8.2	85 (33.60%)
Total (2020)	**1915**	**6.27**	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 October 2020: Notify release #4 – #46.

The month of October saw quite an even distribution of artefacts across all categories (less CIS). Of note, DroneSec saw an increase in number of countries reporting on their purchases of counter drone systems to protect critical installations. This could be due to several of these countries citing intentions and listing tenders to purchase counter drone systems in 2019 and only to award these now. Counter drone systems have been extensively tested for months in several countries before the purchase agreements were made. These systems are essential now with the rise in usage of drones, and along with it, possible safety and risk consequences if not handled properly by operators.

DroneSec also recorded a number of featured reports with a majority of them being failed prison deliveries, followed by incursions and near misses with manned aircrafts near operational airports. However, of note, DroneSec recorded two instances where drones with explosives attached were used with an intention to scare/harm people. This is an act of terror, despite these operators not being affiliated or radicalised in any way.

Category	Number of Artefacts (Jan – Oct 2020)	Compared to Number of Artefacts (Jan – Sep 2020)	Percentage Difference
Featured Incident Reports	136	115	15.44%
Cyber and Information Security	34	32	5.88%
News and Events	375	318	15.20%
Whitepapers and Publications	339	294	13.27%
Counter-Drone Systems	171	139	18.71%
UTM Systems	113	101	10.62%
Drone Technology	213	181	15.02%

The usage of drones rose in the month of October with an above average number of artefacts reporting on trials for BVLOS operations, experimental unmanned corridor and other gadgets enhancing collision avoidance detection and autonomous behaviour.

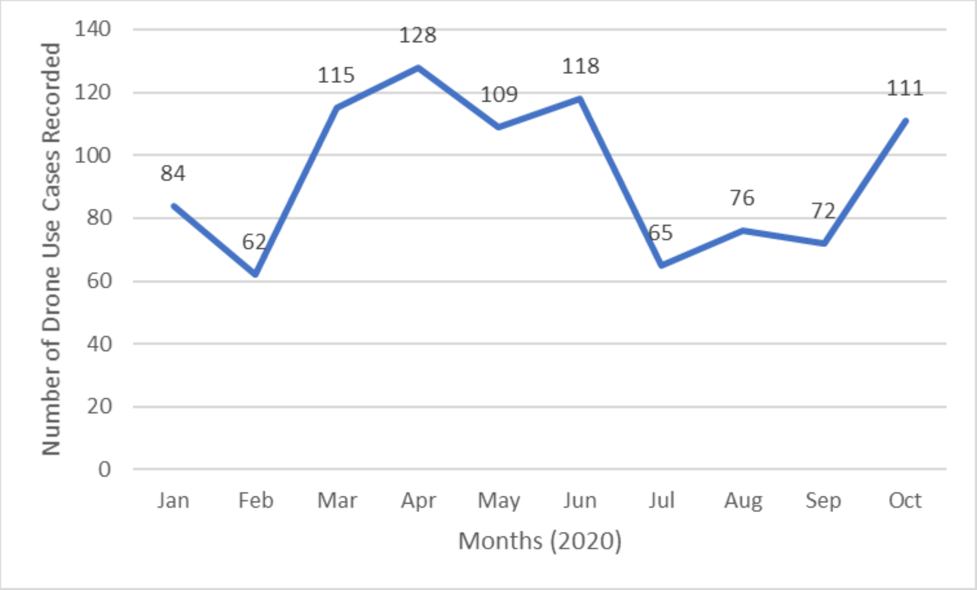


Figure 1: Number of Cases of Drone Usage in the Year 2020 by Months

Incident Summary

DroneSec records news and events that revolve around the use of drones, their innovation, counter measures and development. 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.

The number of drone incidents increased by 21% in the month of October 2020 with a majority of the incidents committed classified as trespass into residences and restricted areas such as prisons.

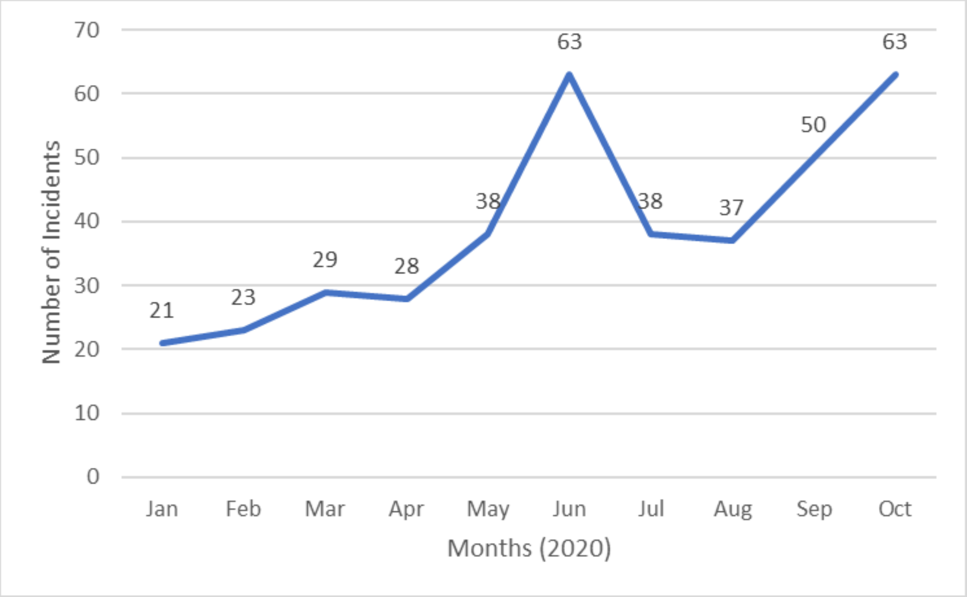


Figure 2: Number of Drone Incidents for the Year 2020 by Months

For restricted areas that have no-fly-zones (NFZs), DroneSec categorised these areas into seven different sectors. All of these categories (less health facilities) have a 10 – 20% increment in drone incursions as compared to September 2020. The increase in number of incidents in areas such as national stadiums, borders and residences shows the need of counter drone systems at these locations, however, due to its large land size, it is impossible to employ adequate drone detection and mitigation systems without a sizeable amount of capital. For now, an incident response plan will serve as an interim solution to manage and handle drone incursions and threats.

Month	Prisons	Events/ Areas of Interest	National Borders	Residences	Aerodromes	Health Facilities	Government Facilities
Oct 2020 -/+ increase	+4	+6	+5	+5	+4	0	+2
Sep 2020	28	36	50	39	32	5	8

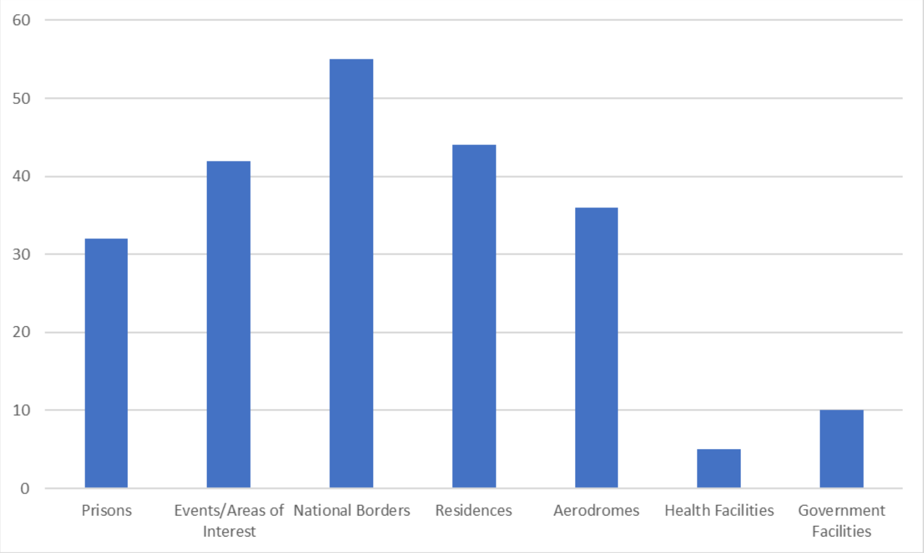


Figure 3: Number of Drone Incidents by Location of Occurrence (since January 2020)

From all the drone incidents that were recorded, DroneSec observed a 58% seizure of drones by law enforcement agencies. These drones were taken down either by kinetic strikes, perimeter defences such as high-rise nets, or in haste to escape, the drones had crashed or gotten stuck in trees. Of the remaining 42%, 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.

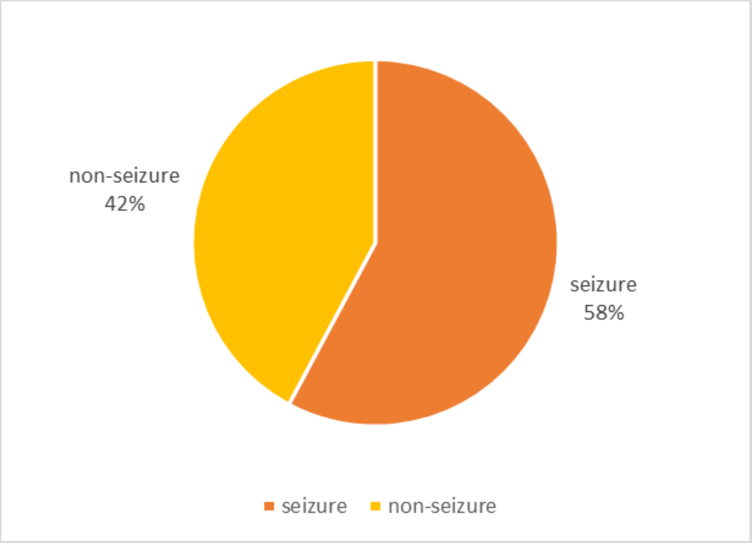


Figure 4: Percentage of drone incidents where the drone system was seized

Conversely, only 28% 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.

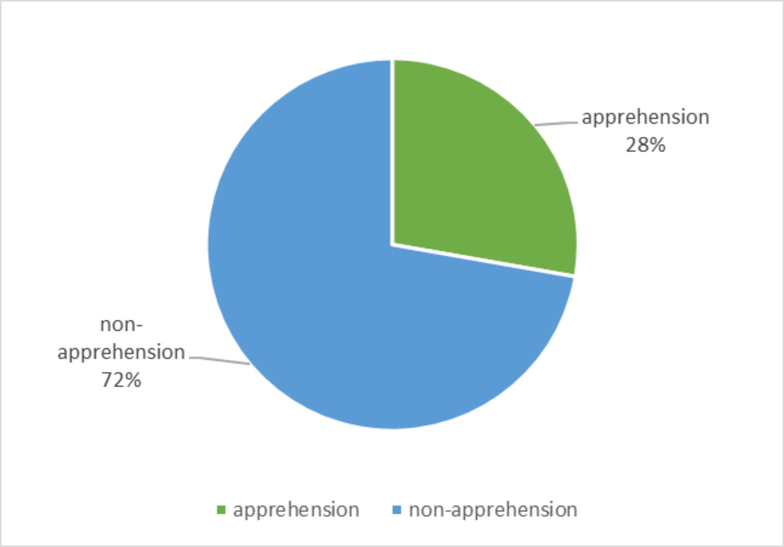


Figure 5: Percentage of drone incidents where the drone operator was apprehended

The difference in percentage on the seizures of drones against the apprehension of the drone operators shows that counter drone systems may only be geared towards the detection and capture of rogue drones. The gap in arresting the operator responsible continues to exist, which should be addressed, otherwise, malicious use of drones will only continue to increase over time.

11% of seized drones aided in the arrest of operators by forensic analysis

DroneSec believe that more errant drone operators could have been discovered if proper tools were available for the extration of drone data, telemetry and flight logs. However, most local law enforcement agencies are currently not equipped to carry out such analysis and have no expertise in doing so. This is another gap which should be addressed in the near future to help lower illegal use of drones and contraband deliveries.

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

Intrusion and Trespass	Priority
Drone operator arrested for flying over Asco nuclear power plant in Tarragona	**P2**

Summary

Law enforcement spotted a drone flying in vicinity of the Asco nuclear plant during a patrol routine and managed to find the operator after a search.

Overview

The Spanish Civil Guard specialising in airspace management and safety, Pegaso, was performing surveillance on critical infrastructures in Tarragona when the security officers spotted a drone flying in the airspace of the Asco nuclear power plant. The drone did not have any identification on it and the officers immediately conducted a patrol in the neighbouring area in search for the operator. The drone pilot was found and was apprehended as he did not possess any permit or approval for flying over the power plant.

Recommendation

DroneSec recommend the military, authorities and law enforcement agencies to be prepared and ready for drone incursions and to have basic preparation measures set in place to respond to such incidents. Aerial threats are hard to detect but basic preparation measures can be set in place to respond effectively. 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 involved should also aim to undertake mock simulations or tabletop exercises together in reacting to such drone intrusions to hone their response, improve communication flow between emergency and rescue agencies and practice on the logging and monitoring of repeated cases.

References

https://elcaso.elnacional.cat/es/sucesos/pillado-dron-central-nuclear-asco-guardia-civil-pegaso_40040_102.html

Intrusion and Trespass	Priority
Pakistani drone continues flying in India despite open fire from Border Security Force	**P2**

[illegible]

Figure 6 - Can't see this report? Get in touch to find out about our premium threat intelligence offerings info@dronesec.com

Safety	Priority
Suspected drone collision with training aircraft at Rand Airport, South Africa	**P2**

Summary

A manned pilot of a light aircraft heard a loud noise after take-off; post assessment shows damage to wing.

Overview

A training aircraft took off at Rand Airport in Gauteng, South Africa, when the pilot heard a loud bang just shortly after take-off. The pilot made a precautionary landing and performed a post flight check. The wing of the aircraft was spotted to have sustained damage and initial conclusions were either a bird strike or a drone strike. However, as there was no feathers or blood on the wing, it was assessed to be a drone strike. Investigations are still ongoing and no further reports were provided.

Analysis

Drone operators must be cognisant of the laws set in place by their country, otherwise there could be a negative repercussion on their actions as a near miss or a direct hit with a manned aircraft could result in potential fatalities. Flight restriction around aerodromes are set in place to ensure safe airspace and to prevent any possible unmanned-manned aircraft collisions as drone operators are not able to accurately assess the height of the drone against the height of the manned aircraft within the same height blocks.

A study from the FAA concluded that drone strikes caused more damage to aircrafts and helicopters than bird strikes due to their hard exterior and LiPo batteries, making drones a real threat to the safety of civil and military aviation. Due to the rigid components of drones, these materials when ingested flew much deeper into the engine and dealt a greater proportion of damage compared to animals.

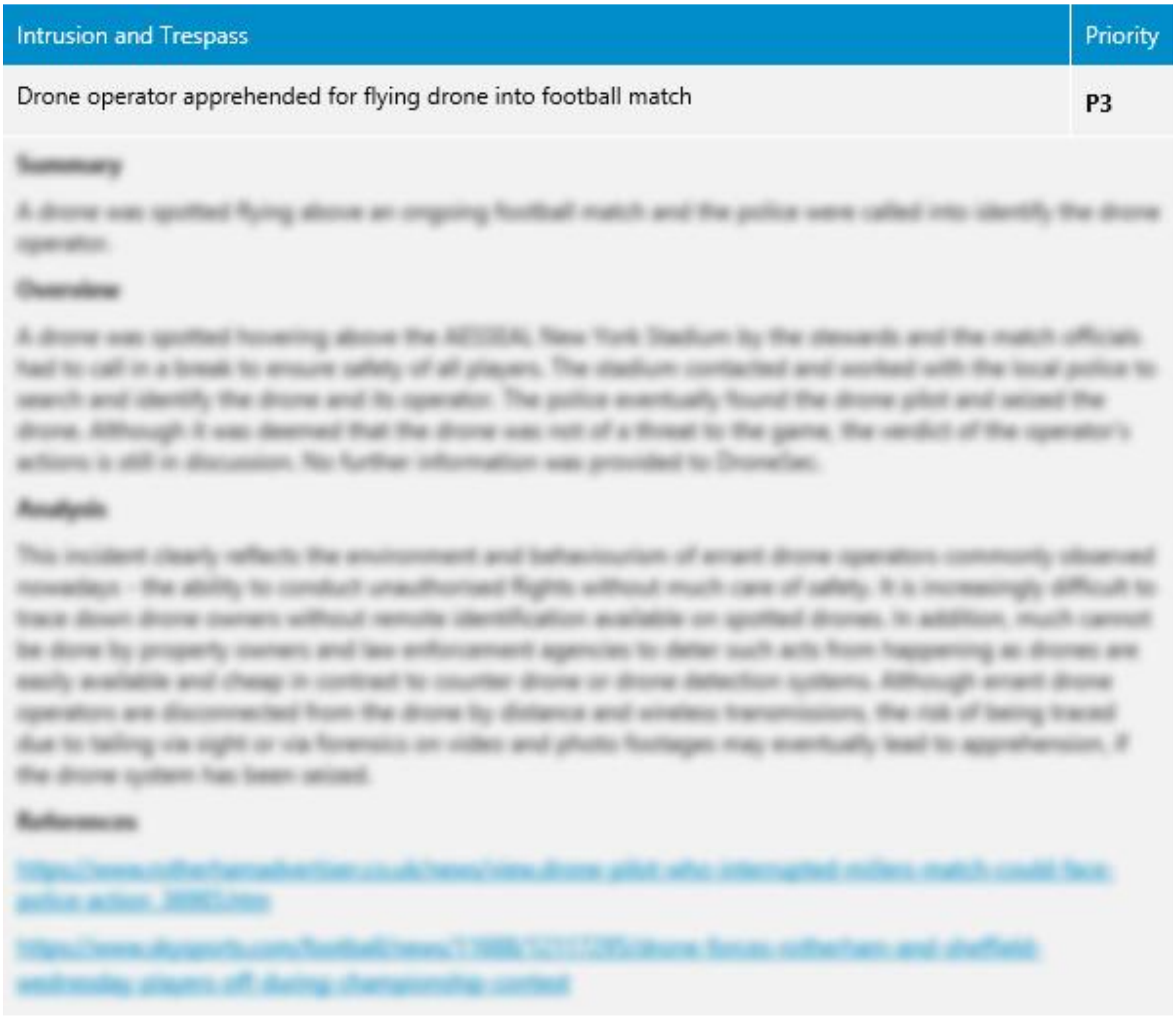
Recommendations

DroneSec recommends all aviation authorities to focus on continuous training for drone operators. Continuous training will ensure that operators do not forget basic aviation fundamentals, drone handling skills and are tuned to basic procedures such as checking for Notice to Airmen (NOTAM), aeronautical charts or flight planning apps before any drone operations.

Concurrently, drone operators are responsible for flying their drones within the limitations imposed by their aviation authorities. It is also their responsibility to be sufficient trained, certified and updated with the latest regulations, procedures and NOTAMs as soon as they become available. Rules and notices on drone operations in certain locality can be found online in the local government aviation websites.

References

https://www.defenceweb.co.za/aerospace/unmanned-aerial-vehicles/suspected-drone-collision-with-aircraft-at-rand-airport/



Intrusion and Trespass	Priority
Drone operator apprehended for flying drone into football match	P3

[redacted]

Figure 7 - Can't see this report? Get in touch to find out about our premium threat intelligence offerings info@dronesec.com

Safety	Priority
Three men arrested for attempting to deliver drugs into Wandsworth jail (UPDATE)	P3

Summary

Forensic analysis on a drone found at a car-chase-crash-scene linked multiple people to narco-drone activities.

Overview

In 2016, a white quadcopter was spotted hovering above Wandsworth Jail by prison security guards and prison guards tailed after the drones which led them to the operator. The drone operator attempted to escape which led into a high-speed police chase following by a fatal crash into a lamppost by the driver which killed his girlfriend.

The drone was carrying narcotics, mobile phones, USB flash drives, cables and a memory card. Through forensics on the drone and mobile phones, law enforcement found that the drone was previously operated by another man and an inmate. All three men were convicted recently for conspiracy along with other unsolved crimes conducted previously as such robbery and theft.

Analysis

Since 2016, DroneSec have seen drone deliveries conducted into restricted areas by organised groups and individuals as they realised that drones are an innovative solution to contraband delivery compared to traditional methods of throwing packages across the walls.

Using drones is a cost-effective technique with reduced risk on being spotted as operators are situated a distance away from the immediate area of operations. This allows malicious users to operate safely with a low risk of being apprehended by law enforcement agencies. Small sized drones can hover in air for a long time at a high altitude, giving it an advantage to stay hidden until it is time to drop the contraband. The drones are small and can be hard to spot with the naked eye giving offenders a good chance to avoid detection and capture by law enforcement agencies.

However, the risk of being traced due to visual sighting or forensics exploitation on a downed/captured drone (via its video and photo footage) poses an exposure risk to the operators. Operators are not impervious from identification as the drone video footage can allow law enforcement to trace the starting and end points of the drone. Facial recognition of the offenders may also be captured within the video, allowing easier investigation against the offender.

References

https://www.dailymail.co.uk/news/article-8897667/Gang-admit-plot-fly-drugs-phones-prison-drone.html?ns_mchannel=rss&ns_campaign=1490&ito=1490

https://www.cps.gov.uk/london-south/news/three-admit-using-drones-smuggle-items-wandsworth-prison

1.4. NEWS AND EVENTS (P3)

U.S. Nuclear Regulatory Commission claims drones not a threat to nuclear power plant sites

https://dronelife.com/2020/11/03/drones-over-nuclear-power-plants-no-threat-says-regulatory-commission/

Hungarian Police investigate journalist use of drones and footages as "illicit data collection"

https://cpj.org/2020/10/hungarian-police-question-journalists-for-illicit-data-collection-after-use-of-drone-footage/

Saudi-led Coalition again destroys multiple Houthi explosive-laden drones

https://www.reuters.com/article/us-yemen-security-saudi/saudi-led-coalition-says-destroyed-houthi-drones-launched-toward-kingdom-saudi-tv-idUSKBN27D1LA

Japan to restrict China's supply of drones due to security concerns

https://uk.finance.yahoo.com/news/wary-security-issues-japans-government-002658457.html

Total of 239 Azerbaijani drones shot down since war with Armenia in September 2020

https://en.armradio.am/2020/10/31/another-azerbaijani-strike-drone-shot-down-in-the-skies-of-stepanakert/

Armenia shoots down Azerbaijan's Bayraktar TB2 drone

https://armenpress.am/eng/news/1033117.html

Armenia shoot down Azerbaijani drone over Stepanakert

https://armenpress.am/eng/news/1033507/

1.5. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P3)

UK National Counter Terrorism Security Office releases guidance on countering drone threats

https://www.gov.uk/government/publications/crowded-places-guidance/countering-threats-from-unmanned-aerial-systems-c-uas

CASA publishes foundational drone safety guide on micro and heavy weight drones, Australia

https://www.casa.gov.au/publications-and-resources/publication/plain-english-guide-micro-and-excluded-rpa-operations

High-tech drones could have neutralised Chinese intrusions at LAC but India didn't have them (commentary)

https://theprint.in/opinion/high-tech-drones-could-have-neutralised-chinese-intrusions-at-lac-but-india-didnt-have-them/532979/

Deadly Taliban attack probably used drone, a worrisome shift (commentary)

https://www.nytimes.com/2020/11/01/world/asia/taliban-drone-afghanistan.html

Public 'more accepting' of commercial drones in wake of pandemic (commentary)

https://www.commercialdroneprofessional.com/public-more-accepting-of-commercial-drones-in-wake-of-pandemic/

1.6. COUNTER-DRONE SYSTEMS (P4)

Pentagon to form a counter drone academy in Fort Sill, Oklahoma, to train all servicemen

https://www.defensenews.com/digital-show-dailies/ausa/2020/10/30/pentagon-is-building-a-school-to-teach-the-force-how-to-defeat-drone-threats/

French Police unit, Raid, utilises CERBAIR CUAS systems, Hydra and Medusa, for national events

https://air-cosmos.com/article/le-raid-et-cerbair-poursuivent-leur-collaboration-23791

Italian Army tests WATSON anti-drone jamming gun by CPM Elettronica at Prometo exercises

https://defence-blog.com/news/army/italian-army-tests-anti-drone-jamming-gun.html

Dutch Army uses Smart Shooter system to shoot down drones

https://defence-blog.com/news/army/dutch-army-uses-cutting-edge-device-to-shoot-down-drones.html

Spanish National Police, MoD, Civil Aviation, MoJ train on protection of aerospace threats

https://www.europapress.es/nacional/noticia-policia-nacional-forma-primer-grupo-agentes-especializados-proteccion-espacio-aereo-20201030193703.html

Countermeasures for Aerial Drones (Publication)

https://us.artechhouse.com/Countermeasures-for-Aerial-Drones-P2065.aspx

1.7. UTM SYSTEMS (P4)

EUROCAE to publish standards on remote ID and ASTM UTM by end 2020

https://www.unmannedairspace.info/news-first/eurocae-remote-id-and-astm-utm-standards-to-be-published-imminently-gutma-utm-standards-webinar/

EHang to initiate UAM trials upon China's announcement of drone experiment zones

https://www.ehang.com/news/695.html

FAA launches BEYOND initiative to tackle BVLOS challenges from 3-year UAS IPP study

https://www.faa.gov/uas/programs_partnerships/beyond/

Astra and Airmarket to conduct cellular-enabled BVLOS UTM trial in Canada

http://astrautm.com/astra-utm-and-airmarket-to-further-enhance-utm-collaboration/

Purdue University and Abu Dhabi work on cyber-secure drone swarms

https://www.hstoday.us/subject-matter-areas/airport-aviation-security/purdue-university-and-abu-dhabi-work-together-on-cybersecure-drone-swarms/

1.8. INFORMATIONAL (P4)

Drone deployed at Port of Antwerp to support enforcement and control operations, Belgium

https://www.transportandlogisticsme.com/smart-sea-freight/drones-to-help-port-of-antwerp-with-control-operations

BAE Systems awarded USD $9M to develop manned-unmanned teaming technologies

https://www.flightglobal.com/helicopters/bae-systems-wins-contracts-to-develop-us-army-manned-unmanned-teaming-technologies/140943.article

1.9. DRONE TECHNOLOGY (P5)

Robotic Research releases Pegasus III, a transformable aerial to ground unmanned vehicle

https://nationalinterest.org/blog/buzz/pegasus-iii-drone-real-life-us-army-game-changer-171463

Vantis announced as state-wide BVLOS network for drones in North Dakota, USA

https://www.suasnews.com/2020/10/north-dakota-announces-vantis-as-statewide-uas-bvlos-network/

Full electric passenger drone, Kite, to ferry between Hong Kong and Macau

https://www.domusweb.it/en/news/gallery/2020/10/30/kite-a-passenger-drone-for-the-hong-kong-greater-bay-area.html

Imperial College London designs dart-shooting drone to aid scientists in deploying sensors

https://www.hansmumm.com/drone-deploys-sensors-by-shooting-them-as-darts/

Stratospheric Platforms Limited and Cambridge Consultant to transmit 5G in for whole of UK stratosphere using drones

https://www.dailymail.co.uk/sciencetech/article-8911237/Worlds-largest-drone-set-transmit-5G-connectivity-stratosphere-using-antenna.html?ns_mchannel=rss&ns_campaign=1490&ito=1490

Researcher gets USD $480,000 grant to develop AI on responding to environment and behavioural changes

http://news.nau.edu/razi-drones/

U-blox high precision technology allows control of 2,198 drones for aerial light show

https://www.gpsworld.com/u-blox-positioning-enables-massive-drone-light-show/

1.10. SOCIALS (P5)

Drone swarms, public perception and drones for first responders (podcast)

http://theuavdigest.com/351-drones-for-first-responders/

Americans warned of missile, drone attacks by US embassy in Saudi Arabia

https://americanmilitarynews.com/2020/10/americans-warned-of-missile-drone-attacks-by-us-embassy-in-saudi-arabia/

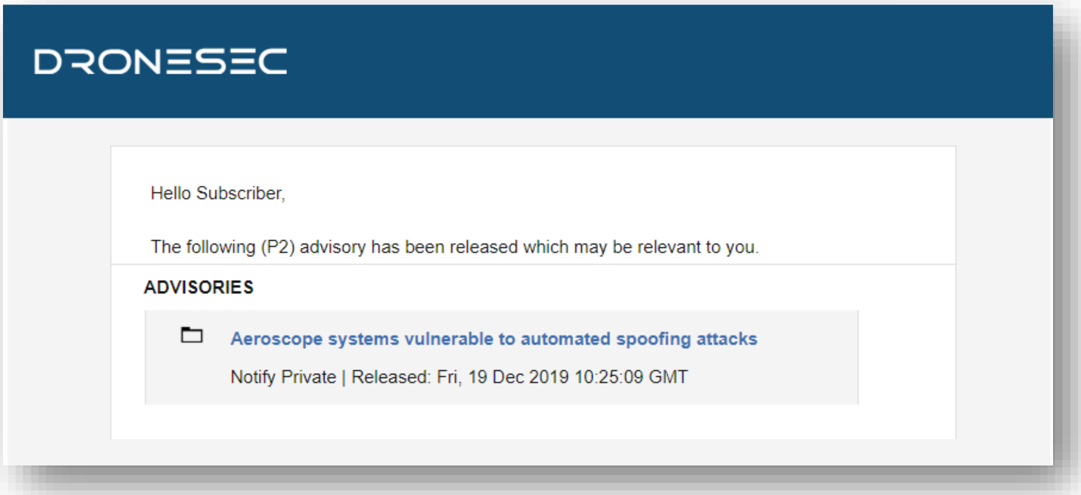
APPENDIX A: THREAT NOTIFICATION MATRIX

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.



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

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

Threat notifications are prioritised based on the following table:

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

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

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

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

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

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

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

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

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

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

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

[4] UTM – Universal Traffic Management System

[5] PSIM – Physical Security Information Management System

[6] OSINT: Open-Source Intelligence from the public domain.

[7] Zero-day: Otherwise known as an 0day or unknown, unpatched vulnerability of which the vendor does not yet know exists.

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

APPENDIX B: SOURCES & LIMITATIONS

B.1. INTELLIGENCE SOURCES

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

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

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

B.2. LIMITATIONS

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

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

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