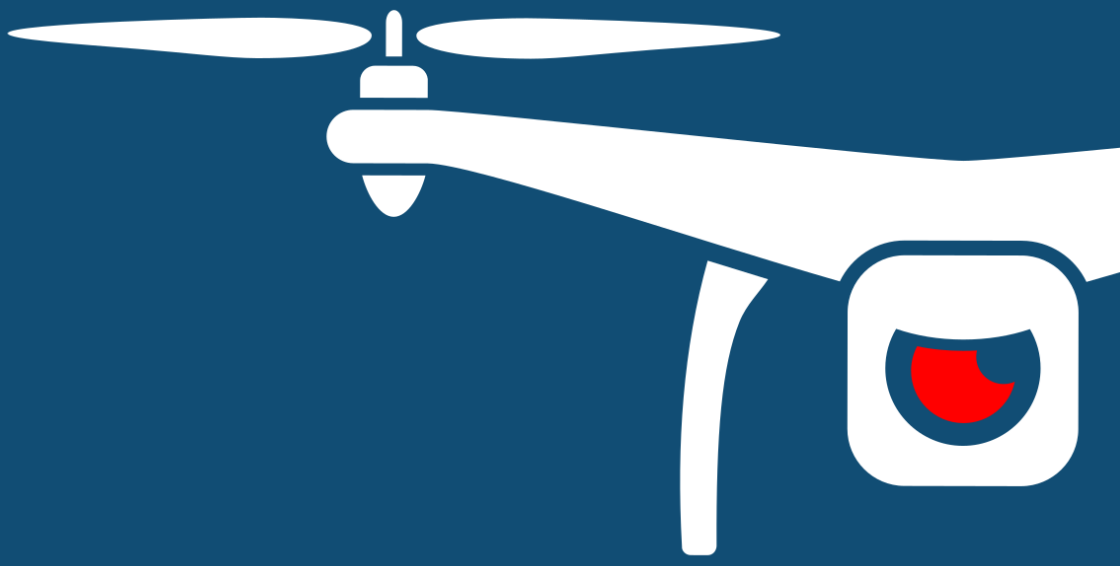
DRONE SEC
A Privasec COMPANY

NOTIFY ISSUE #42 (PUBLIC)

WEEKLY THREAT INTELLIGENCE

30 September 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

It's never a good thing to have to round up a month with a hellish week of drone incidents such as this one. In the past week, we have tracked everything from kamikaze drones (used by Azerbaijani forces to target Armenian troops), the use of a COTS quadcopter to drop explosives in a suburban area, to two airport incursions and continued narco-drones within prison airspace.

We also see a rare report out of Myanmar SEAPAC geographical region where troops allegedly used a multirotor drone to drop explosive ordinance on adversary troops. In Sri Lanka, a man was arrested as part of an organised crime group with drones allegedly being used in a number of innovative crimes. In the US, the Major League Baseball (MLB) organisation continues discussions with FBI and DHS as the drone incursions continue to plague various matches – they are likely discovering the intricacies and status quo of counter-drone regulations worldwide.

Closer to home, Airservices Australia have released an exciting research and analysis position within the National Drone Surveillance Program, DroneShield announce a number of positions available and Mirragin submitted an Australian-owned, sovereign capability for the Australian Maritime Drone Ecosystem (SEA129-5 MUAS).

It's also the end of September, so as we welcome a new month, a monthly look-back takes place. Some interesting figures; a reduction in general drone artefacts, but a 20%+ increase in featured reports. That's quite a fine-tune of signal to noise ratio, something the team is committed to. For all our new subscribers that joined us from the GDSN, please enjoy this report without redactions (Notify customers receive the full report each week).

For Notify platform customers we've added some great research papers available in the Knowledge Base, with the State of Drone Security Report going through its final rounds as we speak.

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 October, 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.

September in Summary

In 2020 thus far, one thousand, six hundred and sixty-two (1,662) 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.

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%)
August	206	6.6	-18 (-8.74%)
September	168	5.6	-38 (-22.62%)
Total (2020)	**1662**	**6.06**	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 September 2020: Notify release #4 – #42.

Although a drop in reported artefacts, we had a 27% increase in featured reports (high priority) within drone incidents in the month of September 2020. A large number of incidents recorded were drone intrusions at major events and deliveries of contraband into restricted areas. Of note, September 2020 had incidents where drones were used to drop narcotics in a public area and to drop explosives to incite fear into neighbourhoods. These items were some of the first of their kind observed for the year.

Category	Number of Artefacts (Jan – Sep 2020)	Compared to Number of Artefacts (Jan - Aug 2020)
Featured	115	90
Cyber and Information Security	32	29
News and Events	318	293
Whitepapers and Publications	294	266
Counter-Drone Systems	139	125
UTM Systems	101	86
Drone Technology	181	157

The usage of drones was at a peak during the months of March to June 2020 when major COVID-19 lockdowns and restricted movements were in place. With regulations easing up in the second half of the year, DroneSec recorded fewer unique cases of drone usage. Drones which were used for delivery and personal reasons during COVID-19 period are less seen nowadays as hobbyists and retail owners start to revert back to their normal lifestyle. Consistent uses of drones that added to the statistics were from terror/rebel groups, government use of drones and larger corporations that had the capacity to expand operations via drone technologies.

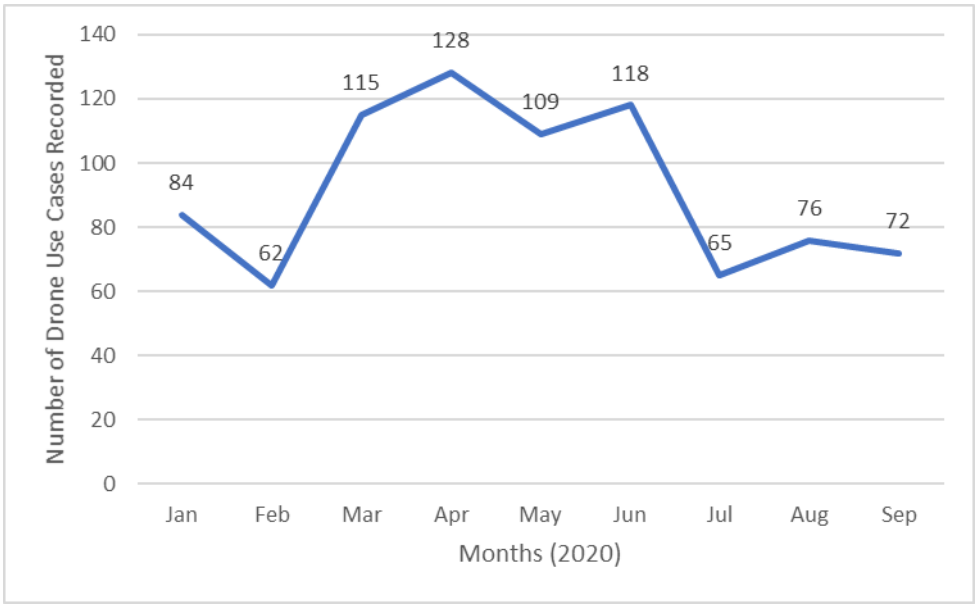


Figure 1: Number of Unique Cases of Drone Usage in the Year 2020 by Months

Incident Summary

DroneSec records news and events that revolve around the use of drones, its 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 26% in the month of September 2020 with a majority of the incidents committed due to trespass and intrusions into restricted areas.

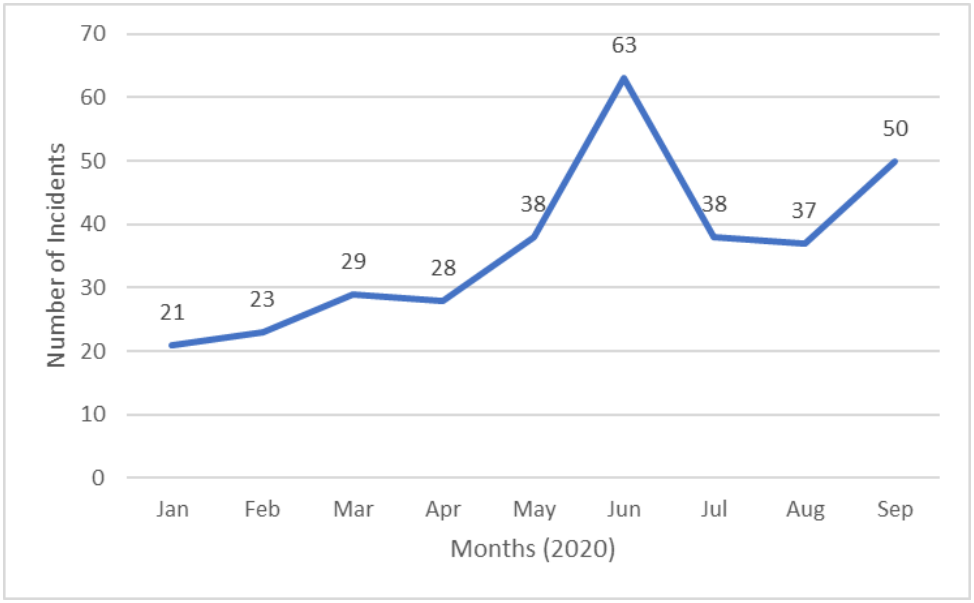


Figure 2: Number of Drone Incidents for the Year 2020 by Months

For restricted areas that have no-fly-zones (NFZs), DroneSec categorised these areas into seven different sectors. For the month of September 2020, event locations, places of interest and government facilities had more than 25% increment in drone incursions as compared to August 2020. DroneSec recorded at least 5 incidents of drones flying into baseball parks which caused matches to halt midway to protect the safety of the players.

Months	Prisons	Events/ Areas of Interest	National Borders	Residences	Aerodromes	Health Facilities	Government Facilities
Sep 2020 -/+ increase	+5	+8	+7	+8	+6	+1	+3
Aug 2020	23	28	43	31	26	4	5

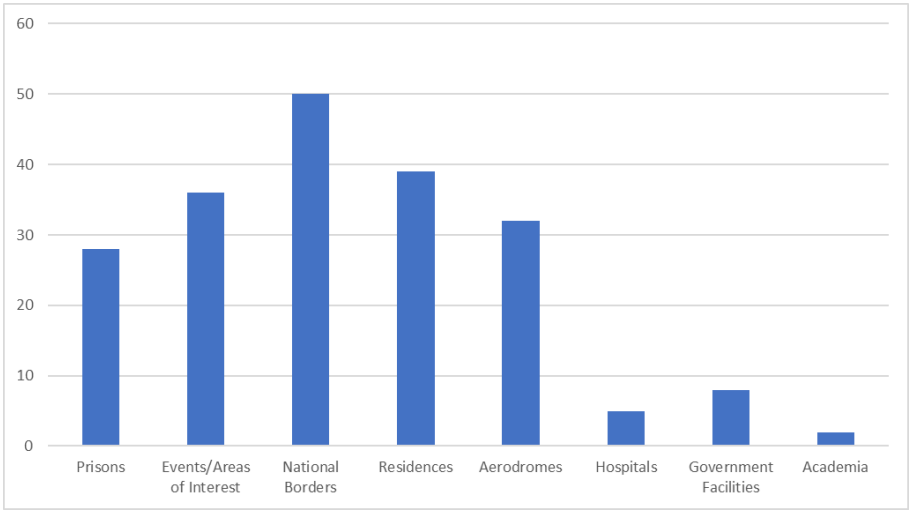


Figure 3: Number of Drone Incidents by Location of Occurrence (since January 2020)

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.

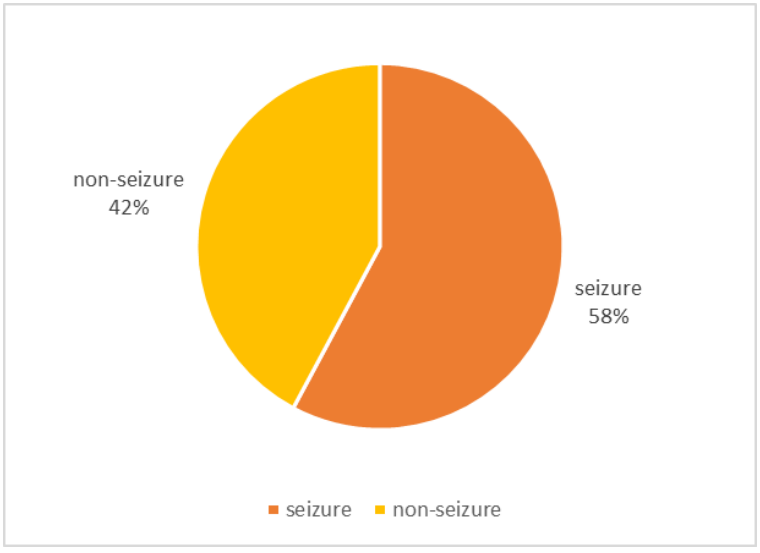


Figure 4: Percentage of drone incidents where the drone system was seized

Conversely, only 27% 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.

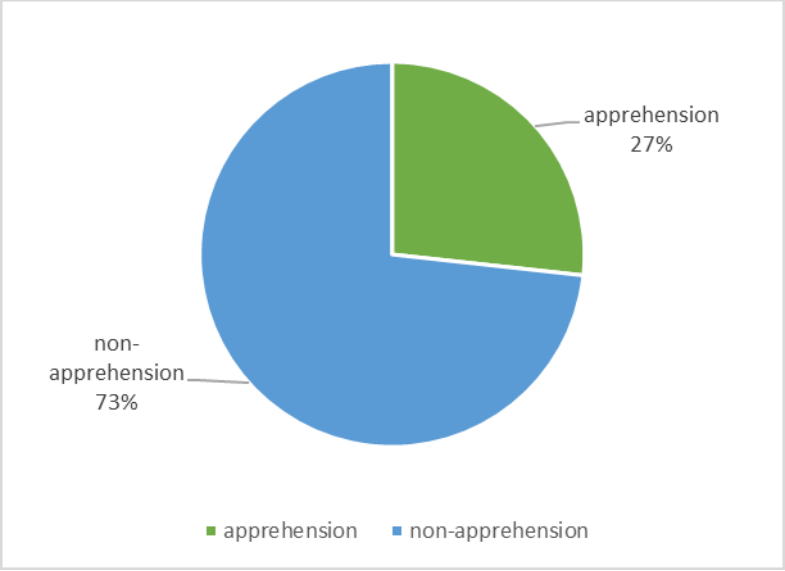


Figure 5: Percentage of drone incidents where the drone operator was apprehended

The stark 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 drone will only continue to increase overtime as drone use grows more popular exponentially.

Only 6% of seized drones aided in the arrest of operators by forensic analysis.

DroneSec believes 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 September 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.

Battlefield Operations	Priority
Multiple UAV incidents involved in conflict between Azerbaijan and Armenian troops	**P2**

Summary

A number of incidents have been attributed to UAV use by Azerbaijan in their offensive against Armenian-held territory. So far, none of the current reports indicate quadcopter or COTS use; however, previous surveillance artefacts the month prior have pointed towards quadcopter use.

Note: This report contains battlefield footage that some might find upsetting.

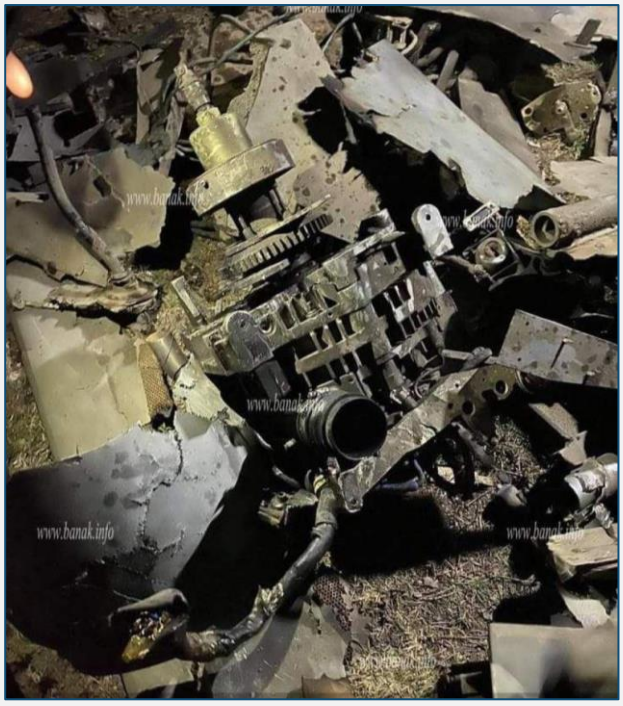
Overview

After weeks of drone surveillance and proxy incidents, an offensive has been launched regarding Armenian-held territory claimed by that of Azerbaijan. Weaponised drone strikes against towns, kamikaze drones against troop positions and anti-tank/artillery actions have been enabled by Azerbaijani drones.

Armenia has claimed 50+ downings of adversary drones, however reports are unclear if these figures include kamikaze-based drones or the method used to destroy them.

Multi-Incident Analysis:

An Azerbaijani drone has struck the Artsakh capital, Stepanakert in what is alleged to be the targeting of civilian populated areas. Some claims are that the drones were 'kamikaze' with mechanical parts found at the blast sites.



- https://twitter.com/Andranik1S/status/1311093693047361542?s=20
- https://zartonkmedia.com/2020/09/29/breaking-news-azerbaijan-kamikaze-drone-bombing-artsakh-capital-stepanakert/

It is also alleged an Armenian bus caught fire after a drone attack by Azerbaijan forces.

- https://twitter.com/spectatorindex/status/1310847025953476609?s=20

Armenian journalists claim they were chased by an Azerbaijan military drone in the village of Nagorno Karabakh.

- https://twitter.com/sharafyan_a/status/1310574306624143360?s=20

The Defence Ministry of Azerbaijan has revealed footage of drone strikes destroying Armenian tanks and artillery.

- https://twitter.com/PressTV/status/1310514350495539200?s=20
- https://twitter.com/Ozkok_A/status/1310528552765452288?s=20

Armenia released footage of Azerbaijani Orbiter 1K UAV downed by armed forces.

- https://twitter.com/ArmenianUnified/status/1310934014526656512?s=20

Armenian air defense systems claim to have downed more than 52 Azerbaijan (Turkish made TB2) drones.

- https://twitter.com/InfoWarriorNews/status/1310910896508727298?s=20

The Azerbaijan army has allegedly been using kamikaze drones to hit Armenian army positions.

- https://twitter.com/RestitutorOrien/status/1311040456248229888?s=20
- https://twitter.com/RestitutorOrien/status/1311053384389197826?s=20

Video filmed from Armenian troops show unsuccessful small arms fire while Azerbaijan drone buzzes overhead.

- https://twitter.com/RestitutorOrien/status/1311050175369146369?s=20

- This is a current Threat Actor assessment and its TTP profile is still being generated –

Recorded Drone Model Types:

- Turkish-made TB2
- Orbiter 1K UAV
- Israeli-made HAROP Azeri

Safety	Priority
Man arrested for dropping explosives via drone near ex-girlfriend's residential home	**P2**

Summary

A series of explosions late at night on Slate Belt Boulevard were found to be linked to a man who owned several weapons and used a drone to drop handmade explosives.

Overview

A string of late-night explosions along Slate Belt Boulevard in Pennsylvania over several months had the FBI conduct in depth forensics on the incident. Similar destructive devices were tested and the culprit's DNA was found in one of the evidences. Law enforcement officers arrested the offender at his home and found multiple firearms, two unregistered drones, of which one was a DJI Phantom 3, and several homemade explosives at his home. The explosives matched the destructive effects found on Slate Belt Boulevard but the memory stick which was used to record the drone's camera video was wiped clean. An investigation was conducted on the

drone app used by the operator which revealed the recorded flight logs of the drone at the incident area.

Analysis

This is the first incident where we see a drone hobbyist using drones to drop explosive payloads in residential neighbourhoods. This is an act of terror with high safety risk, very much alike operations from the Islamic State or the Mexican cartels in asserting dominance and fear. Operating the drone itself has a low skill barrier, however, in this situation, there is some operator experience and domain knowledge required in manufacturing the explosives and creating a drop mechanism for releasing the bomb. Such skills may have been gained from YouTube or other online media.

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.

Recommendation

Currently, it is not possible to provide city-wide coverage of drone detection and counter-drone systems, however, in time to come, regulations and technological advancement would allow cities to be properly equipped against such incidents or threats.

DroneSec recommends the military, authorities and law enforcement agencies to be prepared and ready for such threats and to have basic preparation measures set in place to respond to such incidents. Such aerial threats are hard to detect but basic preparation measures 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.

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

References

https://www.thesun.co.uk/news/12780321/jilted-lover-dropped-explosives-near-exs-home-protection-order/

https://www.mcall.com/news/pennsylvania/mc-nws-pa-jason-muzzicato-bangor-bomber-sentence-20200925-zxpt3uvy6zb5fjjt74mw5oram4-story.html

Intrusion and Trespass	Priority
Flights diverted from Incheon International Airport due to drone incursion, Seoul	**P2**

Summary

Five flights were diverted from Incheon International Airport due to suspected drone activity.

Overview

An unidentified flying object was reported by the Incheon airport officials and a passenger plane and four cargo planes we redirected to another airport due to the incursion. The Korean police manage to trace the drone to a real estate agent who was flying the drone to make a video of an apartment. The drone and the operator were handed over to the aviation authorities.

Analysis

South Korea's Incheon Airport handled the incident well by diverting incoming traffic to avoid the possibility of

a near miss or a mid-air collision with the drone. It is clear that aerodromes and airports are a definite no-fly zone for unmanned drones. However, this operator was unaware of these laws and could have posed a safety risk to manned aircrafts and their passengers.

Recommendations

Incheon airport has a good procedure in mitigating drone incursions and the airport officers were able to react and locate the drone operator quickly. Nationwide registration and identification are a proactive approach to managing traffic between manned and unmanned aircrafts. These systems will allow aviators and law enforcement agencies to (if supported by CUAS activities) prevent further navigation by drones which have infringed regulations. These counter drone measures can help to enforce safe coexistence of unmanned and manned aircrafts, reducing the risk of safety infringements and potential loss of life.

DroneSec recommends for all aviation training schools and federal/state aviation agencies to consider providing fundamental aviation lessons, which are taught to manned pilots, to all drone operators when they are registering their drones. Such training will inculcate the habit of flight safety for drone operators, such as checking for Notice to Airmen (NOTAM) before any drone operations and being ready to handle emergency situations in the event of a malfunction.

References

http://www.koreaherald.com/view.php?ud=20200927000081

Intrusion and Trespass	Priority
Security officers intercept contraband drone delivery at Collins Bay Institution	**P2**

Summary

Prison security officers managed to seize a drone which was carrying contraband into the Institute.

Overview

Collins Bay Institution security officers spotted and intercepted a drone which was flying within the perimeter of the prison. Packages were attached to the drone which contained narcotics and tobacco amounting to $90,000 CAD.

Investigations are still underway and currently, the drone operator is not apprehended yet.

Analysis

This is one of many drone intrusions to the Collins Bay Institution this year.

Using drones is a cost-effective technique with reduced risk on being spotted as operators are situation 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. 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 is time to drop the contraband. Offenders for such acts tend to get away easily as many facilities do not yet possess drone detection or counter-drone systems to mitigate the threat

We are starting to see more drone deliveries across prisons by organised groups as they realise that this is an innovative solution to delivery traditional methods of throwing packages across the walls. The low price point and availability of COTS drones still make drones an easily accessible tool. However, the risk of being traced due to visual sighting or forensics on a downed drone (via its video and photo footages) poses an exposure risk to the operators.

Tracked Actor Category:

Prison Drone Delivery (Local Disruptors)

Motivation and Goals:

- To deliver contraband safely and undetected across the prison walls to supply incarcerated individuals

Tactics, techniques and procedures:

- Use of unmanned systems to separate the distance and risk between operators and contraband payloads
- Use of unmanned systems to conduct reconnaissance and delivery missions
- Use of unmanned systems to overcome physical and personnel security barriers and controls
- Sourcing cheap and available Commercial-Off-The-Shelf (COTS) drones for one-way flights
- Bypassing No-Fly-Zones (NFZ) and restricted airspace by modding and device rooting
- Self-taught in unmanned and contraband-delivery UAS flights and operations
- Using small COTS drones to drop contraband (cellphones, narcotics, weapons ~<2kgs) onto prison grounds, often with purchased or home-made dropping mechanisms
- Utilising counter-forensics techniques by removing SD cards, disabling caching, destroying serial info and disabling the Return-to-Home functionality

Recorded use of drone and equipment types:

- Quadcopters, Multi-rotors
- PGYTECH Air Dropping System
- Homemade contraption with household items (spork, sewing string, fishing string)

Recommendations

Collins Bay Institution is a hotspot for contraband deliveries. In the past, correctional officers have caught multiple offenders attempting to throw packages of contraband across the walls. Today, technology has enabled offenders to use drones for their illicit acts. Collins Bay Institutions and other prisons in Canada have experienced at least six drone delivery incidents this year.

DroneSec recommends all local law enforcement agencies to be prepared and ready for more of such incursions. Though not mentioned on how Collins bay managed to intercept the drone, some facilities may have constraints in deploying similar counter drone solutions; basic preparation measure can be set in place to respond to such incidents. For example, a drone threat management plan and Standard Operating Procedure (SOP) should be drafted to govern the process, people and methodology in handling a drone intrusion.

Organisations should also aim to undertake mock simulations in reacting to such rogue drone incidents to test and hone their response, improve communication flow between agencies and practice on the logging and monitoring of cases. These simulations can aid law enforcement agencies in timing their response, mitigate risk and surface any challenges during the process.

It is also recommended for prisons to have an incident response plan in place for downed/captured drones, such drones offers the law enforcement forensic analysis of the drone's telemetry, data and video footage which could assist in recognising take-off and landing zones and may aid in seizure or prevention of future attempts of drone incursions.

References

https://www.strathroyagedispatch.com/news/local-news/collins-bay-institution-staff-intercept-contraband-drone-drop/wcm/0c040c3a-48d0-455c-82e2-bc968056e4cd

Safety	Priority
Near miss with drone during take-off at Hawera Aerodrome, New Zealand	**P2**

Summary

A drone was spotted flying close to the runway when a manned aircraft was taking off.

Overview

A passer-by spotted a drone flying close to the runway at the Hāwera Aerodrome and noticed a small

passenger plane took off just a short distance away from the intruding drone. The incident was reported to the local authorities but the drone and its operator were not found.

Analysis

This incident clearly reflects the environment and behaviourism of errant drone operators commonly observed nowadays - the ability to conduct unauthorised flights without much risk of being apprehended. It is increasingly difficult to trace down drone owners; in addition, much cannot be done by law enforcement agencies to detect and deter such acts from happening as drones are easily available, cheap in contrast to counter drone or drone detection systems. Although errant drone operators are disconnected from the drone by distance and wireless transmissions, the risk of being traced due to forensics on video and photo footage may eventually lead to apprehended, if the drone system has been seized.

Drone operators must be cognisant of the laws set in place by their country, otherwise there could be a negative repercussion on the innovation within the drone industry and the consequences of their actions as a near miss or a direct hit could result in potential fatalities.

References

https://www.stuff.co.nz/taranaki-daily-news/news/300116106/drone-danger-at-hwera-aerodrome-prompts-warning-from-pilot

Safety	Priority
DJI Phantom 4 crashes into wind turbine due to incorrect height information	**P3**

Summary

During an approved aerial survey, a drone operator flew into a wind turbine because he had incorrect height information.

Overview

A drone operator, who is well versed in conducting aerial surveys, was tasked to operate in an area with wind turbines. The operator used the NATS Drone Assist app as part of his flight planning and risk assessment of the flight, however, the app did not state the height of the wind turbines. The operator searched on the interest for the height which gave him a result of 328ft.

During the aerial survey, the operator flew the drone at 400ft, which was the maximum allowable height for drone operations, across the wind turbine and got struck by the turbine blades. On the United Kingdom's Civil Aviation Authority's aeronautical charts, which is made available to all manned and unmanned pilots, the wind turbine was listed as 413ft in height.

Analysis

In this incident, the AAIB report stated that the drone operator was flying with visual line of sight with this drone. However, it is still difficult to assess the actual height of tall obstacles. Although the drone operator took the correct steps and effort to search for the height of the wind turbine, it is unfortunate that the information he received was wrong which led to the crash. The report also highlighted the safety actions the operator took which is to include referencing to aeronautical charts into his flight planning and risk assessment procedures.

References

https://www.uasvision.com/2020/09/23/drone-crashes-into-wind-turbine-near-bristol/

https://assets.publishing.service.gov.uk/media/5f3cf8818fa8f51741ca5d87/DJI_Phantom_4__reg_na__09-20.pdf

Safety	Priority
Loss of electric power to Yuneec H520 drone due to loose battery in turbulent conditions	**P3**

Summary

A drone crashed onto the ground despite having 97.7% battery power, causing manufacturer to issue update.

Overview

After a prior flight, a drone operator swapped out the battery in his Yuneec H520 drone with a fully charged one. The drone operator proceeded to take off this drone and climb to a height of 45 ft when he noticed the LEDs on the drone was flickering. There were no warnings displayed on the controller and the operator decided to bring the drone back for landing as a precaution.

The LED flickered for the third time and the drone suddenly just fell to the ground, causing damage to the drone, camera and battery. The battery energy level was reflected as 97.7% when the incident occurred.

Analysis

AAIB reviewed the drone's flight data logs and noticed that the log file only had recorded 34 seconds of flight. The logs showed that the drone's pitch attitude had a variance of more than 40 degrees and the roll attitude were of 6 degrees. This could have been an indicate of turbulent weather and Yuneec, after investigation, concluded that the battery became loose during this point in time. The loosening of the battery would have explained the flickering LED lights on the drone.

Yuneec have responded to this incident with an update to its software where take-offs will be prevented when the battery is detected to be loose in its housing.

References

https://assets.publishing.service.gov.uk/media/5f3cf8b4e90e0732e5efe3ab/Yuneec_H520__reg_na__09-20.pdf

1.4. VULNERABILITIES AND CYBER SECURITY (P3)

Kaspersky warns of potential cyber security risk for Amazon's home security drone Ring

https://www.cloudpro.co.uk/it-infrastructure/security/8762/kaspersky-blasts-amazons-indoor-drone-as-a-major-security-risk

1.5. NEWS AND EVENTS (P3)

Myanmar Army used drone to bomb Arakan Army in Kyauktaw, Rathedaung

https://www.arakanarmy.net/post/the-battle-news-and-the-military-offensive-operations-of-the-myanmar-army-in-arakan-in (8th clash incident item)

U.S. Homeland Security raises requirement for department to take down rogue drones

https://www.washingtontimes.com/news/2020/sep/24/dhs-asks-authority-bring-down-drones/

Two dozen explosive-laden quadcopters owned by Mexican cartels found in a raid

https://www.foxnews.com/world/mexico-cartels-narco-tanks-drones-bombs (Update, Commentary)

Sri Lankan arrested for renting out drones without valid licence, drones possibly used for crime

http://www.dailynews.lk/2020/09/28/local/229940/drones-seized-%E2%80%98flower-spraying%E2%80%99-gang-rivalry

Germany imposes ban on sale of aircraft engines to Iran after engines found in Houthi drones

https://www.thenational.ae/world/germany-stops-iran-buying-mini-engines-after-they-were-found-in-houthi-drones-1.1083080

Major League Baseball discuss with U.S. FBI and DHS on drone intrusion prevention measures

https://awfulannouncing.com/mlb/mlb-drones-robust-mitigation-efforts.html

Canadian resident records intruding drone surveilling on his home

https://infotel.ca/newsitem/in-video-kamloops-residents-spot-creepy-drone-watching-their-home-at-night/it77301

Airbus high altitude surveillance and communication drone breaks up in turbulent weather

https://www.itnews.com.au/news/airbus-zephyr-drone-broke-up-in-australian-skies-due-to-unstable-weather-554020

1.6. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P3)

South Korea to ease regulation and allow the use of drones for firefighting operations

https://www.ajudaily.com/view/20200923161957365

U.S. Army leverages AI and drones to fight faster and fiercer (commentary)

https://www.stripes.com/news/us/in-arizona-desert-the-army-prepares-to-fight-much-faster-aided-by-artificial-intelligence-1.646219

The airport and the drone can be friends (commentary)

https://www.aviationpros.com/airports/article/21155169/the-airport-and-the-drone-can-be-friends

The law on shooting down drones (commentary)

https://www.news-gazette.com/news/local/courts-police-fire/the-law-q-a-shooting-down-drones/article_a38e6e87-8bca-5af5-9d8f-17ac2a9b52b8.html

Security analysis of drone systems: Attacks, limitations and recommendations

https://notify.dronesec.com/knowledge (PDF Document: Available for Notify customers only)

Modern methods for detection of unmanned aerial vehicles

https://notify.dronesec.com/knowledge (PDF Document: Available for Notify customers only)

1.7. COUNTER-DRONE SYSTEMS (P4)

Dedrone releases new drone detection sensor, RF-360

https://www.dedrone.com/press/dedrone-introduces-next-generation-of-drone-detection-sensor

DroneShield releases DroneSentry-C2 security dashboard for CUAS management

https://www.unmannedairspace.info/counter-uas-systems-and-policies/droneshield-launches-dronesentry-c2-security-dashboard-to-manage-counter-uas-activity/

1.8. UTM SYSTEMS (P4)

U.S. FAA adds 133 airports for LAANC system for integration of airspace and drone flights

https://www.unmannedairspace.info/latest-news-and-information/faa-adds-133-more-airports-to-nationwide-low-altitude-authorisation-scheme/

India to begin BVLOS drone delivery trials with 13 approved companies

http://www.sfltimes.com/news/drone-delivery-trials-slated-to-start-in-india-this-month

Wing, Uber Elevate, AirMap to develop InterUSS, a drone air traffic management platform

https://www.flightglobal.com/systems-and-interiors/alphabets-wing-division-advances-unmanned-air-traffic-system/140326.article

U.S. FAA grants approval of BVLOS infrastructure inspection to Skyward

https://www.commercialdroneprofessional.com/faa-grants-skyward-staff-permission-to-conduct-bvlos-infrastructure-inspections-from-their-homes/

1.9. INFORMATIONAL (P4)

UK Home Office and MoD to use drones to catch human smugglers across the English Channel

https://www.dailymail.co.uk/news/article-8766543/Jailed-people-smuggler-tracked-drone-Iraqi-36-filmed-eye-sky.html

US Army soldiers in Djibouti train in electronic warfare and CUAS weaponry

https://www.army.mil/article/239319/task_force_bayonet_soldiers_train_in_electronic_warfare

Drone used to find and locate break-and-enter suspects in Trent Hills, United Kingdom

https://globalnews.ca/news/7356095/break-and-enter-arrest-drone-trent-hills/

UK Military using drones to prevent training disruptions on Salisbury Plain, 200 incidents

https://www.itv.com/news/meridian/2020-09-17/drones-deployed-to-tackle-illegal-activity-on-salisbury-plain

Thermal imaging drone helps locate fallen hiker in Otter Rock, Oregon

https://lincolncityhomepage.com/hiker-clinging-to-rock-face-rescued-via-drone-by-depoe-bay-firefighters/

India aims to arm Heron drone with laser-guided bombs amidst tension with China

https://www.forbes.com/sites/michaelpeck/2020/09/29/india-wants-to-arm-its-drones-with-laser-guided-missiles-against-china/#7f809cd3798c

Russia uses drone swarm in military exercise for the first time (commentary)

https://www.forbes.com/sites/davidhambling/2020/09/24/russia-uses-swarm-of-drones-in-military-exercise-for-the-first-time/#2ff819f04771

UK MoD unveils prototype drone with two shotguns, AI vision and real time video streaming

https://www.dailymail.co.uk/sciencetech/article-8784251/MoD-unveils-drone-armed-twin-shotguns-machine-vision.html?ns_mchannel=rss&ns_campaign=1490&ito=1490

Airservices Australia seeks for Drone Surveillance Data and Research Analyst

https://www.seek.com.au/job/50623730?cid=ios-share

DroneShield seek various roles for Counter-Drone capability project work

https://www.droneshield.com/careers

Operator loses control of Parrot drone in flight, possibly due to propeller failure

https://assets.publishing.service.gov.uk/media/5f3cf90a8fa8f51744ded02b/Parrot_Anafi_Thermal__reg_na__09-20.pdf

1.10. DRONE TECHNOLOGY (P5)

Matternet and Japan Airlines partner to deliver drone operations in urban Tokyo

http://www.mttr.net/images/Matternet_Press_Release_JAL_20200922.pdf

University of Illinois-Champaign awarded USD $8M to develop propulsion technologies for drones

https://www.frontiersman.com/arctic-warrior/army-funded-research-may-enable-drones-to-run-on-any-type-of-fuel/article_d281e9d0-fda7-11ea-b99f-1710623095a2.html

General Atomics tests air-launched and air-retrievable drone, Sparrowhawk

https://eurasiantimes.com/us-demonstrates-technology-to-launch-a-drone-from-a-drone-recover-it-back-mid-air/

Singaporean student team develops lifeguard drone to reduce time saving distressed swimmers

https://www.tnp.sg/news/singapore/ite-students-developing-life-saving-drones

Kratos awarded USD $950M to develop capabilities in drone and space technologies for USAF

https://www.airforce-technology.com/news/kratos-wins-usaf-contract-for-abms-programme/

1.11. SOCIALS (P5)

Drone malfunctions at car show, crashes onto vehicle, Texas

https://mavicpilots.com/threads/dji-drone-crashed-into-my-vehicle-at-car-show.98935/

NFL Player Cameron Newton attempts to down drone with ball

https://twitter.com/john_aguero17/status/1311001336456990720?s=20

Warnings provided for drone restrictions for the Glass and Shady fires, California

https://twitter.com/Sarah_Stierch/status/1311014541208227840?s=20

Polish Special Forces to receive 6 micro drones

https://twitter.com/MON_GOV_PL/status/1309070963649241089

Near miss between two drones at Baja rally

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

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.

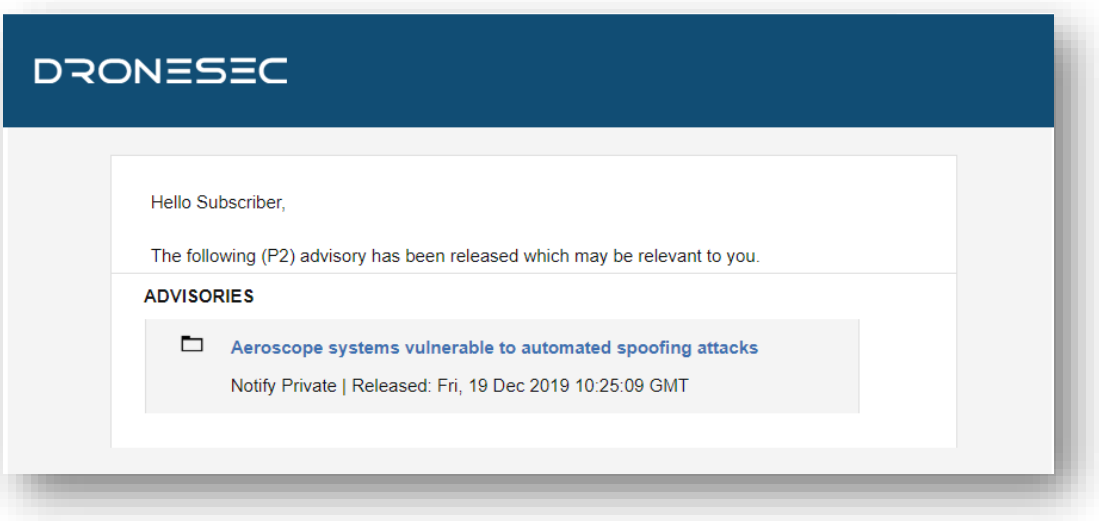


Figure 6 - A threat notification specific to a Notify customer's listed keywords.

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.