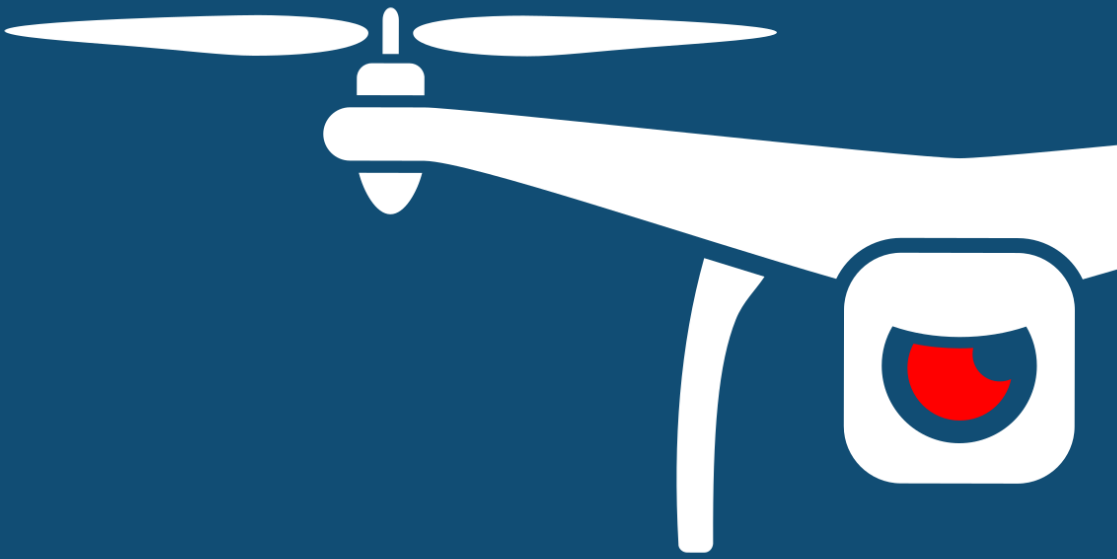
DRONE SEC

A Privasec COMPANY

NOTIFY ISSUE #59 (PUBLIC)

WEEKLY THREAT INTELLIGENCE

27 January 2021 | 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

New to Notify in 2021? This newsletter is a snippet of the information collected, triaged and categorised for statistical analysis in our Notify UAV Threat Intelligence Platform. Built from the ground up to observe drone incidents in real-time, the platform creates a single operating picture for organisations to ascertain local, national and international threats posed by unmanned systems.

This week we see another incident between a helicopter and a drone – a collision occurring in Chile resulting in injury of the pilot. Drone operators manage more than five sorties of smuggled weapons over the Kashmir border before the receivers are apprehended, and a technical report indicates that nefarious GPS jamming is the culprit for the grounding of an entire drone light show's fleet. In Ohio, two men had their narco-delivery drone visually tracked resulting in apprehension and discovery of their operations across multiple prisons in the state. Of note, is a new tactic used by prison delivery groups to deliver contraband into prisons – a mixture of glue and grass to camouflage the package once dropped into the prison yard. In the US – a state-owned drone was repeatedly shot at, with investigations continuing into attribution of the shooter.

Over the last week, the public has been lucky enough to be on the receiving end of URSA's analysis of Counter-UAS testing and evaluation series. It's a terrific read with far-reaching value for a wide range of readers. All these and more in this week's Notify report.

As always, if you have comments or feedback, want to join in the discussion in our slack discussion group, or find the system that captures this information 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.

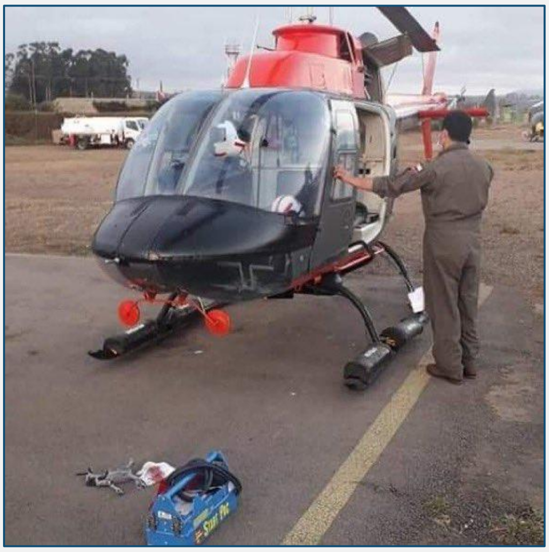
1.2. FEATURED ADVISORIES

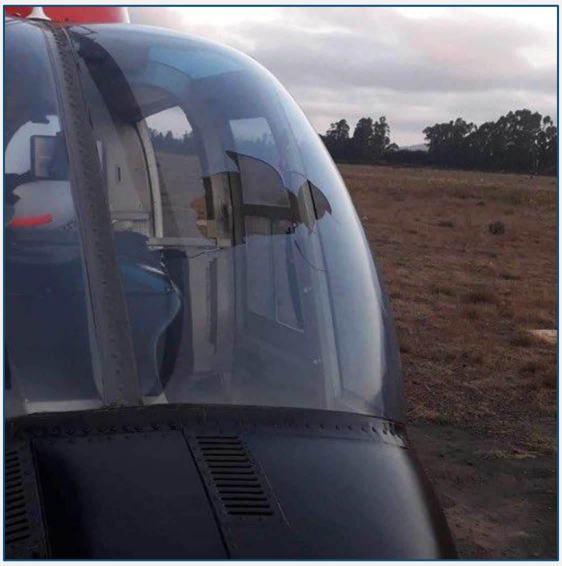
The prioritisation table and its dependencies are explained in Appendix A, and relate to how we filter, analyse and visualise the intelligence we collect.

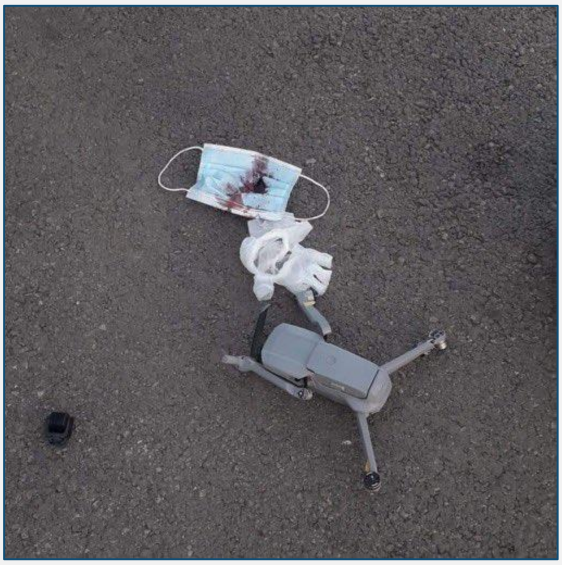
Safety	Priority
Drone crashes into helicopter, breaking the windshield and injuring the pilot	**P2**

Overview

While on a coastal patrol over the coast of Punta de Tralca, a Chilean Navy UH-57B helicopter experienced a collision with a drone. The collision broke the windshield of the helicopter and moderately injured the pilot. The pilot was immediately taken to a hospital for treatment. A subsequent investigation from the Chilean Armed Forces discovered that the crashed drone was a DJI Mavic 2 Pro.







Analysis

- The altitude at which the collision occurred is unknown, however, the report states the helicopter was in a maritime patrol, which may indicate flying close to beach/coastal areas. In some cases, this could occur below 400ft, especially if their surveillance remit included swimmer identification and rescue operations.

- The DroneID and/or operator have not yet been identified, nor is there confirmation from the Navy if forensic analysis is taking place on the drone.

This incident highlights the criticality of unmanned and manned aircraft collisions. Drones are made of hard plastic, contain metal components and batteries which can be more damaging to aircraft compared to that of birds. These components can easily rip apart and break windshields and turbines, creating critical safety issues to the lift and avionics of manned aircrafts.

Without a proper traffic management for unmanned systems, helicopters can fly at altitudes where drones hover at and aircrafts may also encounter errant drone operators flying their drones at thousands of feet up in the sky.

Recommendation

In the meantime, DroneSec recommends all aviation authorities to focus on continuous training for drone operators. Continuous training will ensure that operators do not forget basic drone handling skills (especially during inflight emergencies) 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.

Drone operators should monitor the local CTAF on their airband radio and be aware of common traffic routes where seaplanes or helicopters may be present at low altitudes.

References

https://www.24horas.cl/regiones/valparaiso/helicoptero-de-la-armada-fue-impactado-en-pleno-vuelo-por-un-drone-piloto-resulto-lesionado-4622612

https://twitter.com/scottiebateman/status/1353549260030148608

Intrusion and Trespass	Priority
Militants caught red handed collecting firearms smuggled into India from Pakistan via a drone	P2

[illegible]

Figure 1 - This report is only available to Private Notify subscribers or platform customers.

Intrusion and Trespass	Priority
Two men charged for attempting to deliver drugs into multiple prisons, Ohio USA	**P2**

Overview

Law enforcement officers spotted and traced a drone to a hotel where two men were delivering drugs into prison via a drone.

Overview

Two men were caught delivering narcotics via a drone for the second time into Warren Correctional Institution in Lebanon, Ohio USA. In the first instance, prison security officers spotted a drone delivering contraband into prison ground, which contained narcotics and mobile phones. The package was covered with turf in an attempt to camouflage and conceal when dropped. Security officer followed the drone to a nearby hotel in Monroe but were not able to ascertain the hotel room.

When the offenders launched the drone again for the second time, law enforcement officers were able to obtain a search warrant for the hotel room and managed to apprehend the drone operators and seize the drone. The drone had footages of the drone dropping packages in Warren Correctional Institution as well as two other prisons in Mansfield and Chillicothe.

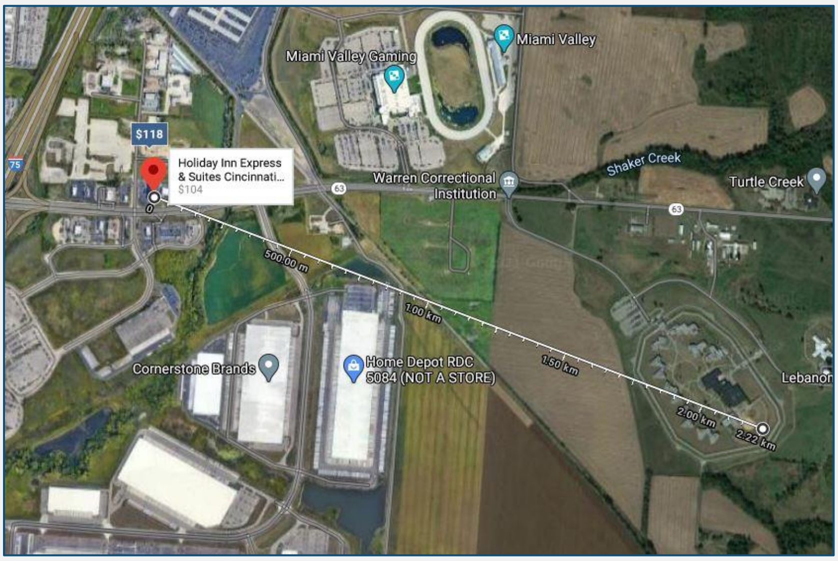
Analysis

- Michael Eugene Russell Williford Jr and Bryan Douglas Shepherd have been indicted.
- The men conducting multiple drone contraband drops at several prisons in the state.
- Visual tracking of the drone led to observation of the operators' launch zone. It is unknown if forensic analysis is being conducted on the systems.
- Highlighted Tactic: Glue was used with turf (grass) to masquerade and camouflage the packages.

The nearest hotel in Monroe, Ohio, is just about 2km away from the backyard of Warren Correctional Institution, where inmates perform daily activities. This distance can be easily managed by drones that are bought off the shelves. Long gone are the days where drones could only fly within line-of-sight, many now being able to fly kilometres away and more if certain modifications are made.

This incident also reflects how small time actors are able utilise technology to their advantage and flout the law. In this incident, the offender has committed drone deliveries into prisons before, inferring that offenders tend to get away easily. This could be attributed to the limitation where many secured or restricted facilities do not possess drone detection or counter-drone systems to mitigate such drone intrusions.

Despite recorded occurrences of such deliveries, many prisons are still ill-equipped against these aerial threats. Drones are small sized and can hover in the air for a long time at a high altitude, giving them an advantage to stay hidden until it is time to drop the payload. It is very easy for prison security officers to miss these dropped packages, hence, giving a boost to the confidence of the drone operators to commit the crime again.



Threat Actor Group

Prison Drone Delivery Group:

https://help.dronesec.com/en/articles/4637701-prison-drone-delivery-groups

Recommendations

DroneSec advocates the needs for a drone threat management Standard Operating Procedure (SOP) or Incident Response (IR) plan where processes, people and methodologies in responding and handling drones and the operators are recorded and followed by all personnel. In this case, maintaining visual tracking and observation of the drone took place in lieu of forensic analysis, as the drone was not initially seized by prison officials.

In addition, changes in security patrols and observation patterns, such as taking more notice of the skies and adjust patrol timings and routes, should be implemented. Drones can surveil patrol routes and schedules, allowing offenders to log these data down and committing the delivery at an off-peak period. Implementing such changes may allow law enforcement agencies to catch these offenders off guard.

References

https://www.houstonchronicle.com/news/article/Indictment-Pair-used-drones-to-drop-drug-15899774.php

Security	Priority
Globe Telecom experiences GPS interference, 20 drones unable to take off for drone show	**P2**

[illegible]

Figure 2 - This article is only available to Private Notify subscribers or platform customers.

1.3. NEWS AND EVENTS (P3)

State drone shot at multiple times during flight to survey and identify hazards to aircraft

https://www.urbanairmobilitynews.com/defence/u-s-state-police-investigate-after-survey-drone-struck-by-gunfire/

Saudi Arabia claims it has intercepted a missile or drone attack by Houthi over its capital

https://abcnews.go.com/International/wireStory/saudi-tv-missile-drone-intercepted-riyadh-75442393

Israeli Defence Force shoots down intruding Lebanese drone crossing international borders

https://www.timesofisrael.com/idf-says-it-shot-down-drone-that-crossed-into-israeli-airspace-from-lebanon/

Jetpack guy flying around Los Angeles could have been a mannequin drone (update)

https://www.thedrive.com/the-war-zone/38802/airliner-pilot-says-jet-pack-guy-over-los-angeles-looked-just-like-this-crazy-drone

Train attempts to disable drone mid-air using water cannon

https://ca.news.yahoo.com/train-almost-takes-drone-water-160002632.html

Drone spotted flying within restricted temple ground in Vrindavan, India

https://www.outlookindia.com/newsscroll/case-registered-after-drone-flown-inside-temple/2017348

1.4. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P3)

Executive Order: Protecting the US from Certain Unmanned Aircraft Systems

https://www.govinfo.gov/content/pkg/FR-2021-01-22/pdf/2021-01646.pdf

Texas Homeland Security Plan: UAS for crit-infra protection, border and smuggling incidents

https://gov.texas.gov/uploads/files/press/HSSP_2021-2025.pdf (pg. 32-33, 80-81)

USA FAA restricts drone flight around Raymond James Stadium in Tampa Bay due to Super Bowl

https://www.faa.gov/news/updates/?newsId=96540&omniRss=news_updatesAoc&cid=101_N_U

Malaysia CAA to publish new directives for drones in February 2021

https://www.thesundaily.my/local/caam-to-publish-new-drone-directive-in-february-YC6325771

2021 is the year the small drones arms race heats up (commentary)

https://www.defenseone.com/technology/2021/01/2021-year-small-drone-arms-race-heats/171650/

Pakistani cross-border terror tunnels, drones are new challenge for security forces in J&K (commentary)

https://www.thestatesman.com/india/pakistani-cross-border-terror-tunnels-drones-new-challenge-security-forces-jk-1502948493.html

Drones - the security temptation (commentary)

https://www.lemonde.fr/economie/article/2021/01/22/drones-la-tentation-securitaire_6067143_3234.html

To defeat enemy drone swarms, troops may have to take the back seat (commentary)

https://www.military.com/daily-news/2021/01/25/defeat-enemy-drone-swarms-troops-may-have-take-back-seat-machines-general-says.html

Counter-UAS Test and Evaluation Series by URSA (Part 1 of 10)

https://ursainc.com/2021/01/15/counter-uas-test-and-evaluation-series/

1.5. COUNTER-DRONE SYSTEMS (P4)

India increases anti-drone measures with sharpshooters, wargaming and radars for air show

https://timesofindia.indiatimes.com/city/bengaluru/bengaluru-sharpshooters-radars-to-prevent-drone-attacks/articleshow/80464351.cms

India's Central Reserve Police Force to acquire Netra V2 drones to combat Maoist operations

https://www.timesnownews.com/india/article/crpf-to-get-micro-uav-a-410-by-may-for-maoist-operation/711207

US Army to evaluate incorporating laser on armoured vehicles to counter adversary drones

https://www.intelligent-aerospace.com/unmanned/article/14195812/laser-counter-uas-uav-drone

1.6. SOCIALS (P4)

Contraband delivery visualised with resulting apprehension of the operator

https://www.linkedin.com/posts/robert-tabbara-568a269_airguard-airspacesecurity-activity-6759891284896362496-ghW-

Chief of Police describes close call with drone flying 100ft away from parachutist

https://www.linkedin.com/posts/activity-6758761613974663168-b_oR/

Drone operator crashes DJI Mavic Air, requests for advice in forums

https://mavicpilots.com/threads/drone-stuck-in-a-tall-pillar-on-commercial-property-what-to-do-next.105552/

1.7. INFORMATIONAL (P4)

Thermal drone helps spot man hiding narcotics within mangroves

https://www.clickorlando.com/news/local/2021/01/21/drone-locates-meth-suspect-hiding-beneath-mangroves-volusia-deputies-say/

Royal Malaysian Air Force unveil prototype UCAV combining DJI Matrice with M4 assault rifles

https://mymilitarytimes.com/index.php/2020/12/13/rmaf-unveils-dji-matrice-ucav-prototype/

Kolkata, India police release e-Tender for law enforcement drones

http://www.kolkatapolice.gov.in/writereaddata/Tender/3549.pdf

1.8. UTM SYSTEMS (P5)

NASA announces UTM technical conference to share lessons learnt from past six years

https://nari.arc.nasa.gov/utm2021tim

Eurocontrol hosts forum to address challenges and opportunities in UAM

https://www.eurocontrol.int/event/eurocontrol-stakeholder-forum-uam

Altitude Angel joins EU Initiative AMU-LED with focus on urban air mobility in Europe

https://www.altitudeangel.com/news/posts/2021/january/altitude-angel-european-partners-realise-future-of-urban-air-mobility/

Nine UK organisations form Airspace of the Future (AoF) Consortium to integrate drone services

https://www.altitudeangel.com/news/posts/2021/january/altitude-angel-takes-flight-with-tech-leaders-to-develop-future-uk-aviation/

Detect and Avoid is the next hurdle out there for BVLOS operations (commentary)

https://www.unmannedairspace.info/news-first/detect-and-avoid-is-the-next-hurdle-out-there-for-bvlos-operations-bob-hammett-onesky/

Seven principles for UAM outlined as framework during Principles of the Urban Sky partnership

https://www.urbanairmobilitynews.com/new-city-projects/drone-think-do-the-seven-uam-principles/

1.9. DRONE TECHNOLOGY (P5)

MBDA use micro-drone as BVOLS spotter with real-time footage for targeting anti-tank missiles

https://www.crows.org/news/548679/MBDA-uses-micro-drone-as-a-spotter-for-its-anti-tank-missile.htm

Steadicopter partners Simlat to provide realistic training simulation for Black Eagle drones

https://www.unmannedsystemstechnology.com/2021/01/steadicopter-partners-with-simlat-for-uas-simulation-training/

How do you know where a drone is flying without a GPS signal? (commentary)

https://techxplore.com/news/2021-01-drone-gps.html

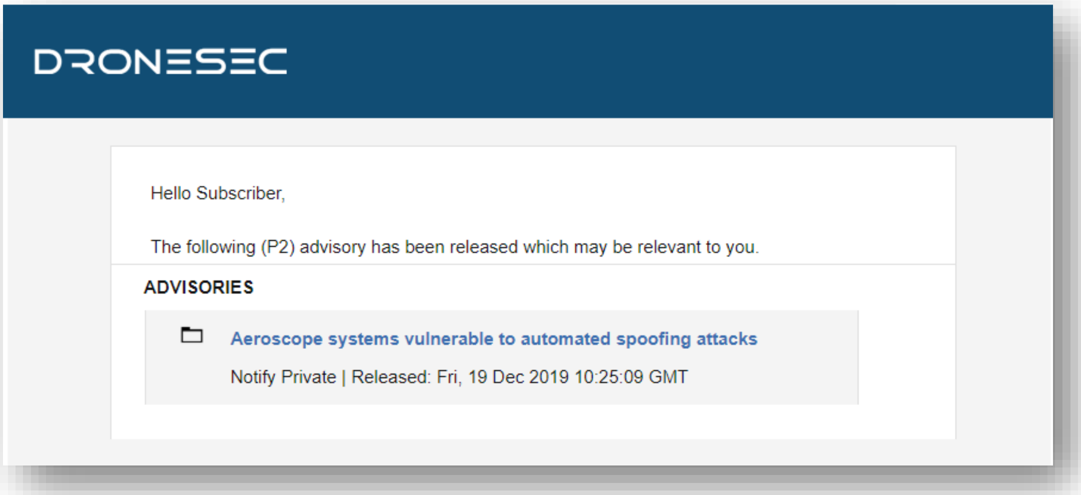
APPENDIX A: THREAT NOTIFICATION MATRIX

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 3 - 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.