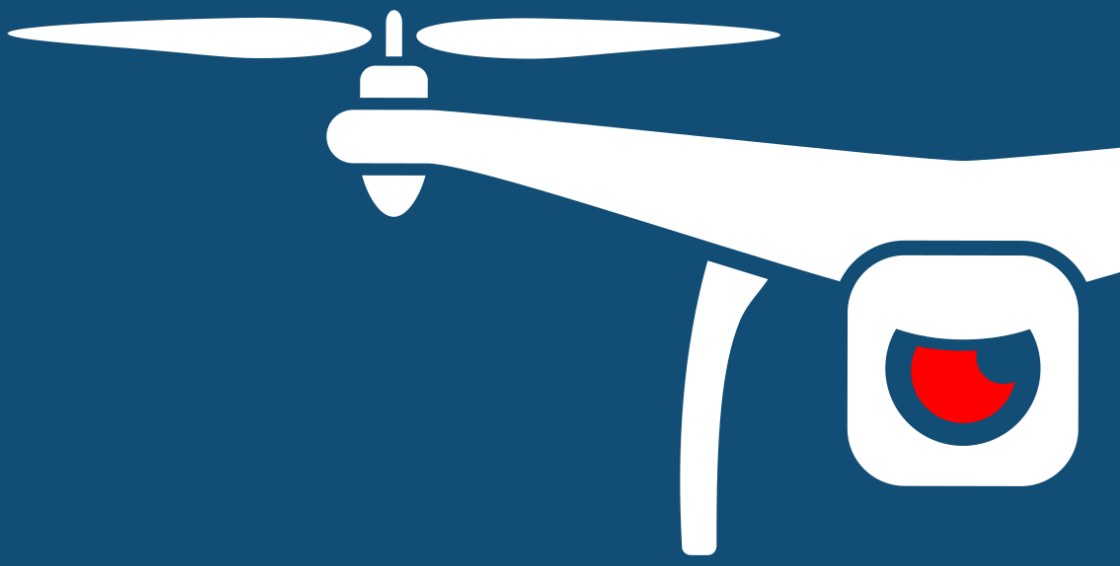
DRONE SEC
A Privasec COMPANY

NOTIFY ISSUE #33 (PUBLIC)

WEEKLY THREAT INTELLIGENCE

29 July 2020 | v1.0 RELEASE



UAS HACKING, HARDENING AND DEFENCE

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

DOCUMENT **CONTROL**

PREPARATION

DroneSec (dronesec.com)

Threat Intelligence Team

Email: info@dronesec.com

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

EXECUTIVE SUMMARY

The countdown is on – September 18th is the official date of the Global Drone Security Network (GDSN) online event. We have various speakers from the CUAS, Law Enforcement, Security Surveillance and Threat Intelligence sectors providing insights into unmanned security-specific topics. We also have a number of interesting reports, white papers and tooling expected to be released during the event specific to the industry.

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

Only a day after bringing attention to Parrot's recent data security and privacy movements, two cyber-security firms conducted an analysis on the DJI Go 4 mobile application. The report is similar in style to River Loop Security's recent analysis of the DJI Mimo app, and yet again draws attention to the data gathered, stored and transmitted by drone manufacturers.

Some news from New Zealand where police have confirmed the terrorist mosque attacker utilised a drone to conduct surveillance and reconnaissance activities against the mosque and its surrounding area by air only weeks before the attack took place. In Australia, another prison drop with apprehension and seizure of the device – an operating protocol (discovering launch sites or near-by vehicles) quickly picking up pace as a successful tactic.

In Syria, regime troops managed to capture a FLIR Black Hornet 3 nano-drone, putting its data security and resilience to the test. Police in Portland, Oregon state that drones are being used by violent protesters to manoeuvre around officers and aid in crimes against officers and the public, prompting the FAA to ban drone flights for a month over the area. The Pakistani army downs their 10th Indian quadcopter drone which was conducting surveillance activities well within the Line-of-Control zone at the border.

Meanwhile in Australia, Department 13 switches from military counter drone activities to enterprises by re-launching with partner Nightingale Security to deliver a joint CUAS and UAS Management platform for commercial operations and compliance. An interesting move for the company in an environment that is consistently looking at joint solutions for UTM/UAM integration with CUAS system functionalities.

All these stories and more in the below report and in our UAS Threat Intel Platform, Notify.

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.

1.2. FEATURED ADVISORIES (P2)

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

Notice to our readers: Featured advisories have provided context and field-based learnings to important incidents within the drone ecosystem. However, with the ever-growing database that we have, DroneSec has moved onto an online repository where artefacts and reports can be tracked, classified and analysed much easier.

Featured Analysis from now on are more comprehensive, wider in spectrum but only available on the Notify platform or to paid subscribers. If you would like continued featured summaries such as the example, please get in touch with us [or purchase a subscription](#).

Intrusion and Trespass	Priority
DJI app analysed for retrieval and transmission of personal data to overseas nationals	**P2**

Intrusion and Trespass	Priority
Four arrested for attempting to deliver narcotics with DJI Mavic 2 into Cessnock Correctional Centre, Australia	**P2**

Summary

Four arrested during surveillance patrol after correctional facility officers spotted a tennis ball loaded with contraband near prison grounds.

Overview

Prison officers spotted a tennis ball loaded with cannabis, tobacco and buprenorphine near the Cessnock Correctional Centre and a surveillance operation was conducted immediately to search for the perpetrator. A man was spotted hiding behind shrubs and was arrested after he tried to resist arrest.

On a subsequent surveillance around the prison vicinity, the prison officers intercepted a vehicle on Pinchen Street with 2 men and 1 woman inside. A DJI Mavic 2 drone, mobile phones, cannabis, cash and buprenorphine was found within the vehicle. The occupants of the vehicle later admitted to their plan of committing a narcotics delivery to the prison using the drone. All four were arrested for trial.

Analysis

This is the second drone-related prison drop we have seen in Australia in the month of July. Using drones are cost-effective technique with reduced risk on being spotted as operators are a distance away from the immediate area of operation(s). 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 secured or restricted facilities do not yet possess drone detection or counter-drone systems to mitigate the growing threat of drone intrusion.

Cessnock Correctional Centre was able to arrest the operators before it happened due to their vigilance in conducting surveillance and patrol around the prison ground and vicinity, otherwise, the offenders might have been able to pull off the act successfully. This incident reflects the growing adaptation of offenders utilising drones to their advantage to carry out illicit operations. Organised crime groups and individuals are realising that drones are an innovative solution against traditional methods of delivering contraband across restricted areas. However, the risk of being traced due to visual sighting or forensics on a downed drone (via its video and photo footage) poses an exposure risk to the operators, which law enforcement officers can make use of.

Recommendations

DroneSec has predicted that prisons in Australia would start to see a rise in such use cases of drones as drone operators are slowly mimicking these incidents that were prominent in United States, Canada and the United Kingdom. DroneSec recommends these agencies to have basic preparation measures set in place to respond to such incidents. Counter-drone systems that allow the detection of drones serve as a good step towards the prevention of drone deliveries. However, these systems are costly and should be acquired based on the needs and requirements of the facility rather than a blanket purchase of sorts.

In addition, a drone threat management Standard Operating Procedure (SOP) or incident response plan should be drafted to govern the process, people and methodology in handling a drone, collecting evidence and responding to potential drone incidents. Agencies should start taking notice of aerial infringements and adjust their patrol timings and routes as these schedules could have already been recorded and logged by the criminal gangs or groups. Security agencies can undertake mock simulations in reacting to such rogue drone incidents to test and hone their response, improve communication flow between participating agencies, practice on the logging and monitoring of drone cases, mitigate risk and surface any challenges faced during the simulation.

Finally, training of security personnel is essential for everyone that could be affected (both directly and indirectly) by rogue or disruptive drones. This training serves to prep effective responses during time critical scenarios and improve communication flow during drone intrusions between involved personnel or agencies.

References

https://www.abc.net.au/news/2020-07-27/drone-drug-drop-thwarted-by-nsw-prison-officials/12496146

https://www.cessnockadvertiser.com.au/story/6851348/drop-by-drone-fails-to-fly-at-prison/

Intrusion and Trespass	Priority
Reports find Christchurch mosque terrorist flew drone over mosque weeks before his attack	P2

1.3. VULNERABILITIES AND CYBER SECURITY (P2)

DJI responses to vulnerabilities mentioned in recent security reports for the DJI Go 4 apps

https://www.dji.com/sg/newsroom/news/dji-statement-on-recent-reports-from-security-researchers

1.4. NEWS AND EVENTS (P3)

Syrian Regime Troops Captured A US Army Black Hornet 3 Nano Spy Drone

https://www.thedrive.com/the-war-zone/34986/syrian-regime-troops-captured-a-black-hornet-nano-spy-drone

Libyan National Army shoots down two GNA Turkish surveillance drones intruding into Sirte

https://english.aawsat.com/home/article/2408336/libyan-national-army-downs-2-turkish-drones-near-sirte

US bans drone flights near federal buildings in Portland, Oregon, for one month citing protesters

https://www.reuters.com/article/us-global-race-protests-drones/u-s-bans-drone-flights-near-portland-buildings-at-center-of-anti-police-protests-idUSKCN24N2L3

Indian ideaForge initiates drone buyback programme to swap out non-No Permission-No Take-off (NPNT) drones with compliant NINJA drones

https://www.ideaforge.co.in/drone-buyback-offer/

Prince Harry and Meghan Markle sue media over drone intrusions and photographs of child

https://www.foxnews.com/entertainment/prince-harry-meghan-markle-sue-paparazzi-invasion-privacy-los-angeles-photos-son-archie

IDF military drone crashed along Lebanon-Israel border during patrol due to technical failure

https://sputniknews.com/middleeast/202007261079987358-israeli-military-drone-crashes-in-lebanon/

Gloucestershire police use 'tech equipment' to arrest man flying drone over Cirencester, UK

https://www.swindonadvertiser.co.uk/news/18609132.police-track-dangerous-drone-flyer/

Rogue drone falls and damages police car during road collision investigation, Houston USA

https://www.click2houston.com/news/local/2020/07/27/drone-falls-on-police-car-at-scene-of-fatal-crash-in-sw-houston-officers-say/

Special Monitoring Mission (SMM) experienced GPS signal interference jamming in Ukraine

For information on the SMM please see 1.11. IN FOCUS – SPECIAL MONITORING MISSION below.

1.5. SOCIALS (P3)

Pakistan Army troops shoot down Indian spy quadcopter intruding into Pandu Sector LOC

https://twitter.com/OfficialDGISPR/status/1287410791789068293

FAA Investigates Drone Sighting Near Teterboro Airport

https://www.youtube.com/watch?v=s6VMkW6JOQg

1.6. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P4)

United States loosen export regulations on sale of military-grade drones and equipment

https://www.defensenews.com/industry/2020/07/24/us-state-department-officially-makes-it-easier-to-export-military-drones/

United States Senate bill to authorise use of drones to identify illicit drug smuggling

https://homelandprepnews.com/stories/34902-senate-bill-would-authorize-use-of-drones-to-identify-illicit-drug-smuggling/

Five US airports to be 'test centers' for UAS detection and mitigation systems over two years

https://nbaa.org/aircraft-operations/uas/faa-moves-toward-regulation-deployment-of-airport-counter-uas-technology/

FCC issues USD $2.8 million fine to HobbyKing for marketing unauthorised drone transmitters

https://docs.fcc.gov/public/attachments/DOC-365706A1.pdf

Australian Army: Unmanned Aerial Systems and the 5th Generation Air Force (commentary)

https://www.williamsfoundation.org.au/post/unmanned-aerial-systems-and-the-5th-generation-air-force-part-one-defining-uas-characteristics-an

Where is air warfare going in the 21st century? (commentary)

https://www.shephardmedia.com/news/air-warfare/opinion-where-air-warfare-going-21st-century/

Is there another contender for drone industry dominance? DJI vs Skydio (commentary)

https://aviationweek.com/sites/default/files/2020-07/AWST_200727.pdf (PDF Document - Pg 16-17)

European Defence Industrial Development Program calls for Counter-UAS proposal Reqs

https://ec.europa.eu/research/participants/data/ref/other_eu_prog/edidp/wp-call/edidp_call-texts-2020_en.pdf (PDF Document, Pg 29 – 33)

Research of Security Routing Protocol for UAV Communication Network

https://www.mdpi.com/2079-9292/9/8/1185/pdf (PDF Document)

Detection and Classification of Multirotor Drones in Radar Sensor Networks: A Review

https://www.mdpi.com/1424-8220/20/15/4172/pdf (PDF Document)

1.7. COUNTER-DRONE SYSTEMS (P4)

Taiwan military prepares for countermeasures against drone swarm threats from China

https://www.taipeitimes.com/News/taiwan/archives/2020/07/27/2003740631

Department 13 re-launches in APAC with C-UAS and Drone Management System offering, partner with Nightingale Security for autonomous surveillance drones

https://department13.com/department-13-enters-australian-airspace-to-deliver-drone-management-excellence/

DroneShield awarded USD$200,000 to install DroneSentry at Grand Forks airbase in North Dakota

https://smallcaps.com.au/droneshield-wins-security-contract-us-air-force/

European Army orders DroneShield's portable counter drone system, RadarZero

https://www.suasnews.com/2020/07/droneshield-order-from-european-ministry-of-defence/

1.8. UTM SYSTEMS (P4)

EVA and Unifly partner to provide Vertical Station solutions on UTM technology and drone infrastructure

https://www.unifly.aero/news/eva-and-unifly-streamline-the-safe-integration-of-drones-from-ground-to-sky

QinetiQ completes first manned and unmanned demonstration with a H125 manned helicopter

https://www.shephardmedia.com/news/uv-online/uk-holds-landmark-mum-t-flight/

Lack of industry standards slows down UTM implementation, Altitude Angel (commentary)

https://www.unmannedairspace.info/emerging-regulations/lack-of-standards-slowing-down-utm-implementation-altitude-angel-seminar/

1.9. INFORMATIONAL (P4)

Chinese President presses military in drone warfare capabilities for aerial attacks and espionage

https://www.scmp.com/news/china/diplomacy/article/3094623/chinese-president-xi-jinping-urges-military-boost-drone

Golden Valley PD defend use of drones for surveillance due to persistent illegal activities (update)

https://www.hometownsource.com/sun_post/community/newhope_goldenvalley/golden-valley-officials-defend-drone-use-at-beach/article_3f9b0db8-cc47-11ea-87f5-2fd2b21c891d.html

Royal Thailand Navy's Orbiter 3B UAV spots oil smugglers off Phuket island

https://www.thephuketnews.com/navy-drone-intercepts-diesel-smuggler-off-phuket-76783.php

Drone used by Barnstable police offices to search for runaway man

https://www.capecodtimes.com/news/20200724/hyannis-man-evades-police-drone-search-by-hiding-in-marsh

Lost hiker in Pagat Cave, Guam, found with help of Drone optics

https://www.postguam.com/news/local/lost-hiker-found-early-sunday-morning/article_3666a8fc-cf11-11ea-b412-3ff6bfd02da1.html

Increased drone activities in Sherborne, UK, police remind residents to adhere to drone laws

https://www.dorsetecho.co.uk/news/18609379.sherborne-residents-report-increase-drone-usage/

Mahwah police drone locates body in Ramapo Valley County Reservation, New Jersey

https://www.nj.com/bergen/2020/07/man-drowns-while-swimming-at-nj-lake-authorities-say.html

Vryburg police call on drone pilot which locates missing body in Hartswater, South Africa

https://www.timeslive.co.za/news/south-africa/2020-07-28-couple-still-missing-drone-finds-daughters-body-in-hartswater/

Vail to incorporate drones as public safety tool for law enforcement and emergency services

https://www.vaildaily.com/news/vail-police-and-fire-departments-add-drone-as-a-public-safety-tool/

Ukraine to purchase more Turkish combat drones, Bayraktar TB2

http://uawire.org/ukraine-to-purchase-additional-batch-of-turkish-bayraktar-tb2-combat-drones

1.10. DRONE TECHNOLOGY (P5)

Singapore researchers create drones that can hover and dart quickly like a bird

https://www.newscientist.com/article/2249612-flapping-drone-can-fly-dart-and-hover-like-a-bird/

Boeing, Northrop Grumman, General Atomics and Kratos win USAF contract to build Skyborg, an AI-enabled drone to aid in manned fighters' warfighting capability

https://www.defensenews.com/unmanned/2020/07/23/four-companies-got-contracts-to-build-the-air-forces-skyborg-drone/

Israeli Defence Force releases video of stick-on-the-wall urban assault drone

https://www.newsrael.com/post/-MCwM84lh7q_fm-HD6-n

Aerodyne and CAB sign to develop drone technology for urban and agricultural sectors

https://aerodyne.group/en/aerodyne-celcom-colaborate.html

1.11. IN FOCUS – SPECIAL MONITORING MISSION

Special Monitoring Mission (SMM) UAV/mini-UAV experienced GPS signal interference in Ukraine by probable jamming near:

Kostiantynivka and Popasna on 21 July 2020

https://www.osce.org/files/2020-07-23%20SMM%20Daily%20Report_0.pdf

Vodiane, Lebedynske, Zhelanne and Holmivskyi on 22 July 2020

https://www.osce.org/files/2020-07-24%20SMM%20Daily%20Report.docx_.pdf

Kostiantynivka and Stepanivka on 23 July 2020

https://www.osce.org/files/2020-07-25%20Daily%20Report_ENG.pdf

Naberezhne, Dokuchaievsk, Krasnohorivka, Dacha, Troitske and Samsonove on 25 July 2020

https://www.osce.org/files/2020-07-27%20Daily%20Report.pdf

Klishchiivka and Popasna on 26 July 2020

https://www.osce.org/files/2020-07-28%20Daily%20Report.pdf

Petrivske and Hranitne on 27 July 2020

https://www.osce.org/files/2020-07-28%20Daily%20Report.pdf

Special Monitoring Mission (SMM) mini-UAV experienced being targeted and shot at in Chernenko, Ukraine, near on 22 July 2020

https://www.osce.org/files/2020-07-24%20SMM%20Daily%20Report.docx_.pdf

Special Monitoring Mission (SMM) mini-UAV experienced being targeted and shot at in Orikhove, Ukraine, near on 23 July 2020

https://www.osce.org/files/2020-07-25%20Daily%20Report_ENG.pdf

Special Monitoring Mission (SMM) mini-UAV experienced being targeted and shot at in Orikhove, Ukraine, near on 24 July 2020

https://www.osce.org/files/2020-07-27%20Daily%20Report.pdf

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.

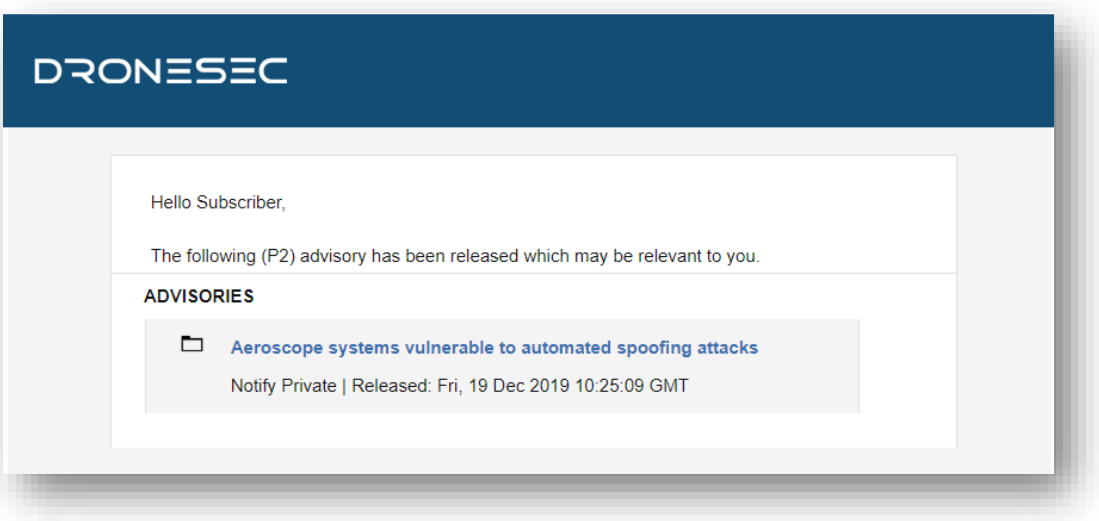


Figure 1 - A threat notification specific to a Notify customer's listed keywords.

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.