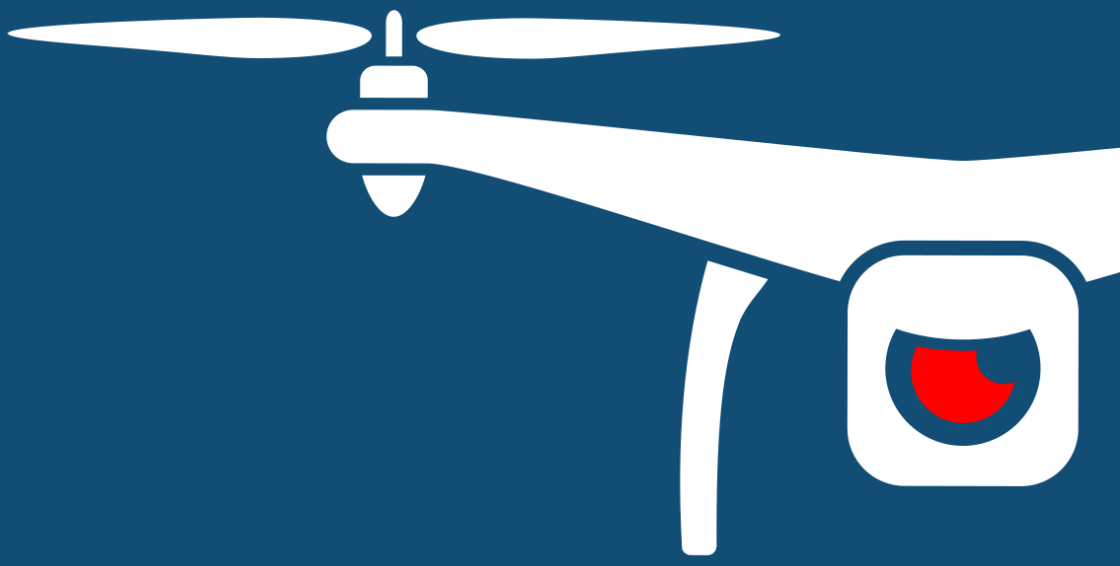
DRONE SEC
A Privasec COMPANY

NOTIFY ISSUE #35 (PUBLIC)

WEEKLY THREAT INTELLIGENCE

12 August 2020 | v1.0 RELEASE



UAS HACKING, HARDENING AND DEFENCE

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

DOCUMENT **CONTROL**

PREPARATION

DroneSec (dronesec.com)

Threat Intelligence Team

Email: info@dronesec.com

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

EXECUTIVE SUMMARY

The Global Drone Security Network is virtual and scheduled for September 18th, 2020. It is now open and available for public registration: https://www.eventbrite.com.au/e/global-drone-security-network-2-tickets-103205143362

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

We are lucky to have such a great network of individuals that are offering to give their time and effort for the community. Our mission is that of sharing practical, relevant, boots-on-the-ground experiences from drone security, counter-UAS and UTM stories and case studies. The event will take place over 8 hours, allowing a global attendance to cover our speakers from Australia, Singapore, Greece, Germany, France, Finland, South Africa and the USA. We appreciate any sharing of the event with your colleagues, as working groups, studies and more will be announced that will be of more benefit with the right people attending.

Another quick update regarding our UAV Threat Intelligence Platform, Notify. A personal thank you to the many users who signed up and use the 'Free' tier subscription on a daily basis. However, to better service our paying customers, and to give insight of the full-features available, the following changes are taking place:

- 'Free' tier will be discontinued and replaced with 'Premium' tier trials, for fixed length.
- All weekly UAV threat intel newsletters (like this one) will continue unchanged.

This means you will experience the full capabilities the platform has to offer (minus the tailored reports/intelligence from our analysts) but for a limited time only. We are actively reaching out to subscribers to make them aware of this change and setting up demonstrations on using the full-featured trial version. 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.

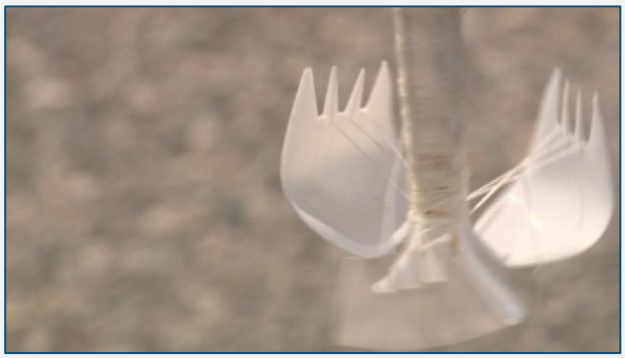
Intrusion and Trespass	Priority
Drone with homemade spork mechanism found on building of Richmond Justice Center, USA	**P2**

Summary

Richmond police officers spotted a crashed drone at the top of the Richmond Justice Center with a homemade contraption for carrying contraband items.

Overview

Richmond City police officers spotted an intruder attempting to climb into Richmond Justice Center via a ladder and decided to investigate the scene. Officers seized a crashed drone on the building and realised that the drone had a contraption attached, made from several easily obtainable household items. A clamp, made from 2 sporks, were tied together by a string and attached to the base of the drone. This clamp was able to carry items and be delivered by the drone. Although no contraband item was found, officers suspected that the drone was used for contraband delivery into the prison, but the drone operator was not successful in doing so. The drone operator was not located.



Analysis

Drones used for narcotics and contraband delivery is a pressing issue in the United States since 2015. Offenders are constantly growing more creative in committing crimes, utilising new and cheap technologies like drones to their advantage to carry out illicit operations. The low price point and availability of drones becomes an innovative solution against traditional methods of delivering contraband across restricted areas. Using drones also reduces the risk of being spotted and apprehended by law enforcement agencies as operators are situated a distance away from the immediate area of operations.

However, delivering contraband items requires a bit of knowledge and skill; offenders have to think of ways to be able to carry the items, travel amidst environmental conditions and release the items at the appropriate time. Failure to secure or release the items correctly will result in a failed delivery along the way, or to an unintended recipient. DroneSec has recorded several tools and mechanism that were used by small time

offenders and most of them were homemade contraptions which required the recipient to manually remove the contraband from the drone. DroneSec has also recorded the use of PGYTECH dropping system used in one of the incidents as part of the delivery tool.

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/Equipment:

- Quadcopters, Multi-rotors
- PGYTECH Air Dropping System
- Homemade contraptions with household items

Recorded Contraband/Crime:

- Narcotics (cannabis, marijuana, tobacco, steroids)
- Communication devices (cell phones, SIM cards, batteries)
- Equipment (syringe)
- Weapons (saw blade)

Recorded Area of Operations:

- Collins Bay Institution, Canada
- Joyceville Institution, Canada
- Mansfield Correctional Institution, United States
- Forest Prison, Belgium
- Wymott Prison, United Kingdom
- Alexander Maconochie Centre, Australia
- Bovingdon Prison, England
- Longuenesse Prison, France
- Hays State Prison, Georgia
- Erlestoke Prison, England

Recommendations

Counter drone systems are a good way to deter or prevent against drone intrusion, however, the cost of these systems and legal restrictions may be a blocker. DroneSec recommends law enforcement agencies to have basic preparation measures 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 threat. These plans and procedures can aid to govern the process, people and methodology in handling a drone intrusion, collecting forensic evidence and responding to potential drone incidents / drone operators in a predetermined radius around the prison grounds.

As drones can also be used for surveillance, 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. Unexpected or a change in patrol schedule will catch drone operators off guard and provide opportunities for the seizure.

In cases like this incident where the drone has crashed, forensic analysis of the drone's telemetry would be incredibly useful, potentially aiding in the launch location of the drone. Event analysis from the drone data and video footage could assist in recognising patterns and trends (such as origin of flight, time of day etc.) providing possible modus operandi of other operator(s) and may aid in seizure or prevention of future attempts of drone incursions.

Lastly, DroneSec recommends training of security personnel, operators and any workers that could be affected (both directly and indirectly) by drones. This training will aid to hone responses and improve communication flow during incidents and allow all participating agencies to respond effectively during time critical scenarios and mitigate possible risks from drone threats.

References

https://www.wtvr.com/news/local-news/sheriff-someone-tried-to-use-drone-to-smuggle-contraband-into-jail

Intrusion and Trespass	Priority
CASA issues request on finding large drone operating near Sydney airport, Australia	**P2**

Summary

A drone was spotted flying close to a passenger aircraft in Sydney Airport and authorities are looking for eyewitnesses identify the drone operator.

Overview

During an approach for landing at Sydney Airport, the pilot of a passenger plane spotted a quadcopter flying close to the aircraft at an altitude of about 1,200 metres (about 4000 feet). The sighting was reported to the airport and the Australian Civil Aviation Safety Authority (CASA) issued an appeal to the public on finding the incident drone. DroneSec did not receive any further news on the appeal and the drone operator and drone were not apprehended or seized thus far.

References

https://australianaviation.com.au/2020/08/wanted-casa-hunt-rogue-drone-flying-near-aircraft/

1.3. VULNERABILITIES AND CYBER SECURITY (P3)

Consumer UAV Cybersecurity Vulnerability Assessment Using Fuzzing Tests

https://arxiv.org/pdf/2008.03621.pdf (PDF Document)

Drone Penetration Testing and Vulnerability Analysis (RSA Conference) (PDF document available in the Notify Knowledge Base)

1.4. NEWS AND EVENTS (P3)

Israel downs drone at Mount Hermon while on high alert for possible Hezbollah attacks

https://www.timesofisrael.com/idf-small-drone-entered-israeli-airspace-from-lebanon-brought-down-by-troops/

ISIS reveal photos of captured AeroVironment RQ-20B Puma drone and attempts to reverse engineer it

https://www.hstoday.us/subject-matter-areas/airport-aviation-security/isis-shows-seizure-study-of-u-s-made-drone-in-sinai/

Trespassing drone shot down by anti-aircraft guns at Khmeimim Airbase, Syria

http://www.sana.sy/en/?p=199604

Tourist reports large drone spotted outside bathroom window in Canada

https://www.coastreporter.net/news/local-news/police-report-large-drone-seen-hovering-outside-bathroom-window-1.24181716

Colorado man fined for flying drone and crashing into a silo in Snyder County, USA

https://www.pennlive.com/news/2020/08/man-pleads-guilty-fined-125-for-flying-drone-into-snyder-county-silo-opening.html

Employees spots drone hovering outside of office window at Gordon Avenue, Georgia

https://www.timesenterprise.com/news/local_news/drone-peering-into-windows-under-investigation/article_12750873-b36a-50e3-bb62-ad7184c891d7.html

Man arrested for illegal driving possessed drone and narcotics with intent to deliver

https://www.wboy.com/news/crime/officers-find-man-in-possession-of-drone-used-to-deliver-controlled-substances-during-traffic-stop-in-marion-county/

Food delivery drone crash lands during delivery attempt, Chicago USA

https://www.dailymail.co.uk/news/article-8615799/Hungry-customer-watches-drone-delivering-14-fail-just-feet-office-window.html

Turkish drone strike kills two Iraqi Kurdistan Workers' Party (PKK) commanders

https://english.alarabiya.net/en/News/middle-east/2020/08/11/Turkish-drone-strike-kills-Iraqi-border-guards-Iraq-military-says.html

India's military propose to equip Heron UAVs with bombs and missiles armament

https://economictimes.indiatimes.com/news/defence/armed-forces-push-case-for-arming-israeli-drone-fleet-with-laser-guided-bombs-missiles/articleshow/77445721.cms

1.5. SOCIALS (P3)

IDF deploy "roof-knock" drone strikes to warn Gaza citizens of imminent drone missiles

https://twitter.com/manniefabian/status/1293318098305658886

Weaponised UAV bombed Rafah Airport, Southern Gaza Strip

https://twitter.com/GazaNewsOfficia/status/1293319567507369991

DroneSec to hold second Global Drone Security Network on UAS, CUAS, UTM security

https://www.meetup.com/GDSNetwork/events/272396742/

Defence Aviation Safety Authority (DASA) UAS Symposium on 22 October 2020

https://www.defence.gov.au/DASP/Docs/ConferencesAndSeminars/Seminars/DASAUnmannedAircraftSystemsSymposium.pdf

ICE71 Webcast: From Hollywood to Real Life – The Threat of Drones (Webinar)

https://ice71.sg/events/event/live-webcast-from-hollywood-to-real-life-the-threat-of-drones/

1.6. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P4)

Japan impose ban on drone flights over 15 USA military sites for security reasons

https://www.japantimes.co.jp/news/2020/08/07/national/japan-ban-drones-us-bases/#.XzC7bSgzZPY

30nm radius "No Drone Zone" imposed over Charlotte Convention Center on August 24, 2020

https://www.wbtv.com/2020/08/10/republican-national-convention-designated-no-drone-zone-by-federal-officials/

India's Ministry of Defence to impose import embargo on drones for military December 2020

https://www.medianama.com/2020/08/223-military-drone-import-ban-india/

Whitepaper suggests UAS may prevent theft and increase security of construction sites

https://repozitorium.omikk.bme.hu/bitstream/handle/10890/13431/013.pdf?sequence=1 (Page 22)

Pakistan gets Chinese DJI drones to monitor Indian ships (commentary)

https://www.sundayguardianlive.com/news/pak-gets-chinese-drones-monitor-indian-ships

South China Sea Crisis: Beijing's drone proliferation ignites tensions in disputed region (commentary)

https://www.express.co.uk/news/world/1320607/south-china-sea-news-drone-technology-Beijing-us-crisis

Army advances learning capabilities of drone swarms (commentary)

https://www.army.mil/article/237978

Drone crash due to GPS interference in UK raises safety questions (commentary)

https://www.forbes.com/sites/davidhambling/2020/08/10/investigation-finds-gps-interference-caused-uk-survey-drone-crash/#1ddcac76534a

Bringing non-cooperative drone traffic into UTM solutions (commentary)

https://www.aviationtoday.com/2020/08/11/bringing-non-cooperative-drone-traffic-into-utm-solutions/

Congress probes US reliance on Chinese spy drones (commentary)

https://freebeacon.com/national-security/congress-probes-u-s-reliance-on-chinese-spy-drones/

Drones for evil purposes: This is how the police should stop them (commentary)

https://translate.google.com/translate?hl=en&sl=no&u=https://www.uasnorway.no/droner-til-onde-formal-slik-skal-politiet-stoppe-dem/&prev=search&pto=aue

Whitepaper: Drone and Pilot Controller Detection for Critical Infrastructure (AeroDefense)

(PDF document available in the Notify Knowledge Base)

United States Drone Laws, August 2020 Update (911 Security)

(PDF document available in the Notify Knowledge Base)

Countering IED-UAV: A Long-Term Simulation-Based Study by NATO CIED COE

(PDF document available in the Notify Knowledge Base)

1.7. COUNTER-DRONE SYSTEMS (P4)

Korea's Agency for Defense Development reveals use of laser and EMP weapons to target drones

https://www.donga.com/en/article/all/20200806/2142796/1/Laser-beam-and-EMP-launchers-to-fight-against-drones

US Army selected CACI's CORIAN drone detection and neutralisation system

http://investor.caci.com/news/news-details/2020/CACIs-CORIAN-Selected-for-the-Defense-Departments-C-sUAS-Mission/default.aspx

1.8. UTM SYSTEMS (P4)

PrecisionHawk awarded two patents on collision avoidance technologies for UTM systems

https://www.precisionhawk.com/blog/utm-patents-awarded

SqwaQ demonstrates LTE drone communication technology which can resolve UTM obstacles

https://www.unmannedairspace.info/latest-news-and-information/sqwaq-develops-lte-comms-module-which-obviates-need-for-utm-restrictions/

Hyundai Air Mobility and Urban-Air Port invest USD $1.5b to develop UAM infrastructure in UK

http://www.koreaherald.com/view.php?ud=20200806000726

1.9. INFORMATIONAL (P4)

UK Police forewarn public on possibility of drone use for burglaries and thefts

https://www.kentonline.co.uk/dartford/news/fears-burglars-are-using-drones-to-scope-out-homes-231691/

Western Australia Police to acquire 40 DJI Phantom 4 and Matrice 210 drones for daily operations

https://www.australiantimes.co.uk/news/wa-goes-big-on-aerial-policing-capability-using-drones/

Russia to enlist S-70 Okhotnik ("Hunter") combat drone to fight along manned aircrafts by 2024

https://www.popularmechanics.com/military/aviation/a33548209/russia-hunter-combat-drone/

Drone aids Derbyshire Police to apprehend drug dealer and 8 other suspects

https://www.dailymail.co.uk/news/article-8596617/Dramatic-moment-police-drone-tracks-drug-dealer-leaps-window-caught.html

Elbit's Hermes 900 military drone crashes into Israeli desert during test flight

https://www.swissinfo.ch/eng/israeli-drone-ordered-by-swiss-army-crashes-during-test-flight/45951158

1.10. DRONE TECHNOLOGY (P5)

uAvionix releases 978MHz and 1090MHz Detect and Avoid ADS-B receiver for drones

https://uavionix.com/introducing-pingrx-pro/

Herotech8 deploys drone-in-a-box solution at Cranfield Airport for automated airfield inspection

https://www.suasnews.com/2020/08/drones-used-to-conduct-automated-inspections-at-cranfield-airport/

University of Alabama in Huntsville gets USD $1.1M to lead research on drones for disaster preparedness and response

https://www.waff.com/2020/08/06/uah-gets-m-grant-lead-drone-disaster-preparedness-research/

Botlink receives four year nationwide wavier from FAA for operations over populous

https://botlink.com/blog/2020/8/6/botlink-receives-four-year-nationwide-waiver-for-operations-over-people

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.

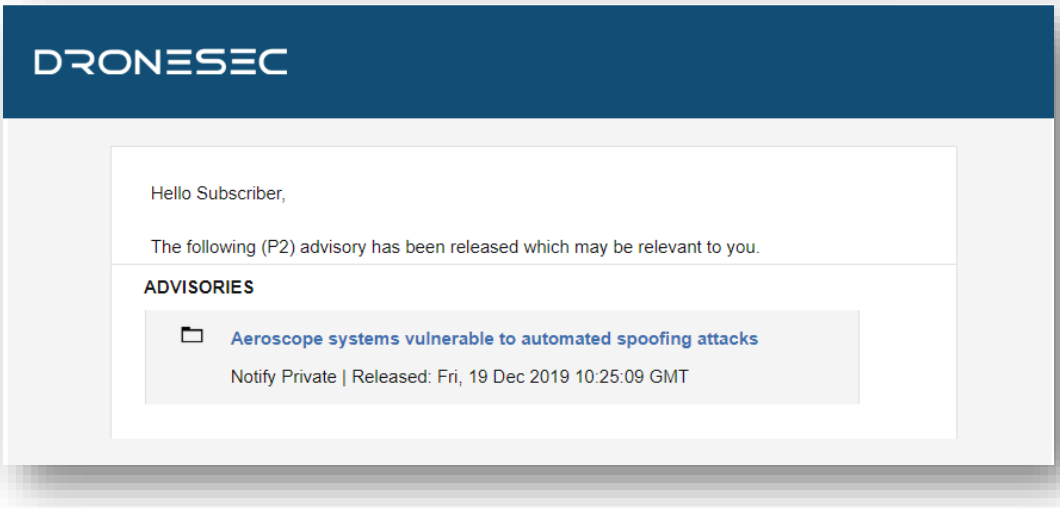


Figure 1 - A threat notification specific to a Notify customer's listed keywords.

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.