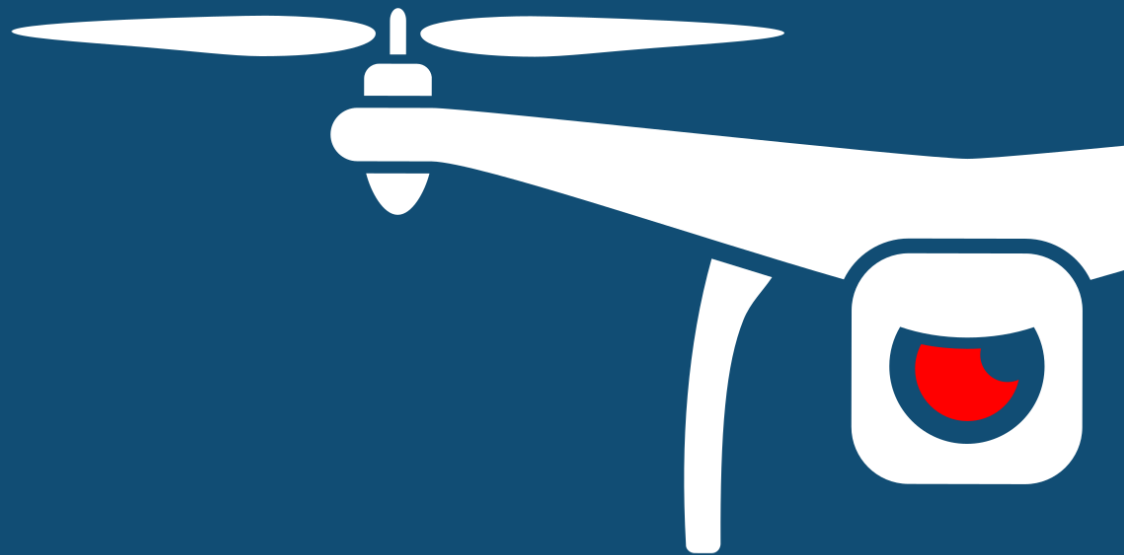DRONE
SEC
A Privasec
COMPANY

NOTIFY ISSUE #17

WEEKLY THREAT INTELLIGENCE

8 April 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)

DOCUMENT **CONTROL**

EXECUTIVE **SUMMARY**

DroneSec Notify Threat Intelligence Platform (TIP) - Dark Mode

Its webinar week this week at DroneSec HQ with a live presentation for Sphere Drones aimed at drone organisations (recording located here) and a more technical-based presentation aimed at security participants of the upcoming virtual conference ComfyConAU on Friday 7:30pm AEST. It's a great time to focus our efforts online, when the team was initially meant to be stretched between Norway, Cambodia and Singapore for working groups, conferences and talks this month.

COVID-19 news and chatter continue to dominate the headlines but some key frameworks and whitepapers released this week show the significant energy investment in managed drone programs worldwide. Furthermore, Christopher Church has announced the next INTERPOL Framework for Responding to a Drone Incident will be released in the coming weeks – the updated version will be available here on Notify.

Today we take a closer look at what might be the first of its kind – usually drone incidents involve airports or correctional facilities; in this issue, we explore what it means for medical services when their industry is disrupted (and with it, their patients). Investigations continue with this one as police still unable to locate the suspect.

We want to again thank one of our contributors for providing an update to the IDF drone downing incident, providing a photograph to zone in on the perceived make and model. These are important aspects of artefacts which allow us to continually track and catalogue the types of drone Counter-Drone and Law Enforcement Agencies (LEA) can expect to respond to. Another update sits within a story we reported in December; rival gangs used drones to drop swine-flu infected meat into pig pens, infecting the hogs. As an update, its revealed one of those hog farms installed Counter-Drone technology, disrupted GPS/GLONASS signals and got a visit from their communications authority – bit of a twist!

Finally, we look at the incredible effort by the UK RAF and MoD in putting together a swarming drones squadron aimed at "network-enabled drones capable of confusing and overcoming enemy air-defence systems" – however, much of the information points to the utilisation of existing technologies rather than a bespoke platform.

For our non-customer subscribers, we're closing off BETA applications to the Notify platform on April 24th. This will be a discounted opportunity to use the platform as 'early access' where we are looking for partner organisations to test, feedback and report their use for general improvements. For example, one reoccurring suggestion was the implementation of a "dark mode" (as above).

-   *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.

Kicking it all off, we're delivering our first few rounds in PDF format. In the next few weeks, we'll continue to roll out platform access to ensure we can sustainably support our current client needs with relevant, actionable information within the context of DCU.

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 (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.

Security	Tags	Priority
Drone flies into rescue helicopter landing zone during medical evacuation operation	Drones, Safety, Emergency Services	P2

Summary

A personal drone flew into the landing zone of a medical helicopter, causing a delay in medical evacuation.

Overview

A DJI Mavic drone which hovered in the vicinity of a helicopter landing spot caused a delay in an evacuation operation to Vanderbilt Hospital in Limestone County, USA. The helicopter pilot spotted the drone just before they were about to land and had to wait for the drone to leave the area before it could do so safely. Medical evacuations are time essential and a delay in delivering appropriate responses could cause have a significant impact in a life-threatening situation. Police are still looking for the drone operator.

Analysis

It is now fairly common to observe malicious drone operators flying into restricted areas due to ignorance or disregard of aviation law governing drone flights. Despite public broadcast on what can and cannot be legally undertaken with drones, there are still many operators who continue to disregard these for a variety of reasons. However, this instead has a negative affect on the innovation within the drone industry as regulators enforce more stringent rules – sometimes, affecting the legitimate and commercial drone operators over controlling the malicious.

In addition, studies from the FAA have concluded that drone strikes cause more damage to aircrafts and helicopters than bird strikes due to their hard exterior and LiPo batteries – as a result, rogue drones near aircraft are a real threat to the safety of civil and military aviation. Due to the rigid components of drones, their materials (when ingested into the demonstration aircraft) flew much deeper into the engine and dealt a greater proportion of damage compared to animals. It is important that drone operators are cognisant on the consequences of their actions as a near miss or a direct hit could result in potential fatalities.

Recommendation

UAS Traffic Management (UTM) systems are a proactive approach to managing indirect incidents between drones and aircraft – when the flight is not intentionally malicious. UTM systems enforce safe coexistence of unmanned and manned aircrafts, reducing the risk of safety infringements and potential loss of life due to medical aviation delays. Drone operators should be cognisant with the laws of their country and have the appropriate licenses if required. Operators should aim to keep themselves up to date or relevantly trained before operating a drone.

For law enforcement and medical aviation bodies where counter-drone systems aren't readily available, undertaking table-top simulations or exercises to counter for scenarios like these are essential. Furthermore, they should have a Standard Operating Procedure (SOP) or Incident Response Plan in play to mitigate potential delays, overcome landing preventions and quickly involve the appropriate law enforcement bodies.

Training is essential for non-operators working in a field that could be affected (both directly and indirectly) by rogue or disruptive drones. DroneSec educates seasoned and newcomers with webinars and training courses which cover drone operation fundamentals, laws and security aspects.

References

- https://www.enewscourier.com/news/local_news/officials-drone-pilot-interfered-with-injured-toddlers-transport/article_c4047932-749e-11ea-b106-8f331bd3f1e8.html

1.3. NEWS AND EVENTS (P3)

UK Royal Air Force activates drone swarm Squadron 216 for overcoming air-defence systems

https://www.janes.com/article/95245/uk-stands-up-swarming-drones-development-unit

Russian reconnaissance UAV shot down and apprehended by Ukrainian troops

https://www.ukrinform.net/rubric-defense/3000100-informnapalm-drone-downed-in-donbas-in-service-with-twelve-russian-army-units.html

US Air Force conducts its 34th drone strike, targeting Al-Shabaab terrorists in Somalia

https://sofrep.com/news/us-drone-strike-in-somalia-whacks-5-al-shabaab-terrorists/

FAA investigate "Anti-COVID drone task force" violating aviation regulations

https://thehill.com/policy/technology/491410-faa-investigating-mystery-drone-telling-new-yorkers-to-socially-distance

IDF shoot down Hezbollah drone flown over border from Lebanon (UPDATE – photos)

https://www.timesofisrael.com/idf-shoots-down-drone-from-lebanon-says-it-was-flown-by-hezbollah/

Chinese pig farm Counter-Drone equipment taken after GPS signal disrupts flights (UPDATE)

https://www.telegraph.co.uk/news/2019/12/23/chinese-pig-farm-attempts-block-criminal-drones-signal-jammer/

1.4. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P3)

Standardisation Roadmap for UAS by US ANSI's UASSC open for comments

https://www.prnewswire.com/news-releases/ansi-draft-standardization-roadmap-for-unmanned-aircraft-systems-version-2-released-for-comment-301033469.html

https://share.ansi.org/Shared%20Documents/Standards%20Activities/UASSC/UASSC_20-001_WORKING_DRAFT_ANSI_UASSC_Roadmap_v2.pdf (PDF File)

European Union Aviation Safety Agency proposes opinion on regulatory framework for manned and unmanned aircraft operations

https://www.easa.europa.eu/document-library/opinions/opinion-012020

US DHS urges drone operators to avoid flying near agriculture planes; crops deemed as essential service during pandemic

https://www.capitalpress.com/sponsored/uas-operators-cautioned-to-not-disrupt-food-supply-chain-during-covid-19-pandemic-by-interfering/article_ca28ce00-7500-11ea-a299-370f4ec848f4.html

Australian aviation body CASA defers mandatory drone registration to September 2020

https://www.casa.gov.au/about-us/news-article/remotely-piloted-aircraft-registration-and-accreditation-–-further-assistance-industry

Scheduling drone charging for multi-drone network based on consensus time-stamp and game theory

https://www.mendeley.com/catalogue/ef96a6ce-38fc-391f-b09b-10973d1a2974/ (PDF available to Notify customers)

1.5. COUNTER-DRONE SYSTEMS (P4)

US Air Force deploys Raytheon's anti-drone swarm laser weapon overseas for field testing

https://taskandpurpose.com/military-tech/air-force-laser-weapon-fielding

Counter-Drone Solutions for Civilian and Military Use – Drone Radio Show (Podcast)

https://www.youtube.com/watch?v=5Dlp9JBCvSg

1.6. UTM SYSTEMS (P4)

ANRA Technologies launches SmartSkies, an authorisation platform for execution and management of drone operations in controlled and uncontrolled airspace

https://markets.businessinsider.com/news/stocks/anra-technologies-launches-smartskies-drone-airspace-authorization-platform-for-airport-control-zones-and-sensitive-areas-1029068113

Altitude Angel launches UTM mobile app for safety information on drone pilots in Netherlands

https://www.internationalairportreview.com/news/114608/lvnl-drone-safety-information-mobile-app/

1.7. DRONE TECHNOLOGY (P5)

Doodle Labs develops mesh broadband router for unmanned systems for 116km BVLOS ops

https://doodlelabs.com/about-us/news/doodle-labs-releases-external-smart-radio/

Chinese firefighters use six drones to put out a blazing 10-storey building in 15 minutes

https://www.dailymail.co.uk/news/article-8180019/Chinas-firefighting-drones-extinguish-blazing-10-storey-building-minutes.html

https://youtu.be/WFqThcMIN7A

Kollam police purchase 350 drones to monitor and enforce COVID-19 lockdown in Kerala, India

https://english.mathrubhumi.com/news/kerala/police-use-350-drones-for-surveillance-in-kerala-1.4666160

Rakuten Mobile and AirMap to collaborate for drone inspection on telecom base stations

https://telecom.economictimes.indiatimes.com/news/japanese-telco-rakuten-mobile-to-use-drone-to-carry-out-base-station-inspection/75006267

Drone dispersed disinfectants conflict over efficiency of response vs health hazards

https://www.reuters.com/article/us-health-coronavirus-disinfection/mass-disinfections-to-combat-coronavirus-pose-another-health-hazard-idUSKBN21I1PB

Ireland begins drone delivery operations during pandemic lockdown with Manna Aero

https://www.forbes.com/sites/simonchandler/2020/04/03/coronavirus-delivers-worlds-first-drone-delivery-service/#1d9600f64957

Doha Ministry of Interior, Qatar, launches COVID-19 awareness via DJI Mavic drone broadcast

https://www.thepeninsulaqatar.com/article/02/04/2020/Drones-to-broadcast-coronavirus-awareness-message-in-Qatar

Drone in Ahmedabad to alert cops when citizen flout the 1.5m social distancing rule

https://timesofindia.indiatimes.com/city/ahmedabad/drones-to-alert-cops-with-beeps/articleshow/74957734.cms

Uttar Pradesh government deploy drones to monitor religious activities at mosque

https://www.outlookindia.com/newsscroll/now-drones-to-monitor-friday-prayers-at-noida-mosques/1790047

Assam Police, India, deploy drones and arrest 75 people violating lockdown

https://www.aninews.in/news/national/general-news/assam-police-deploy-drones-to-monitor-situation-in-guwahati-amid-lockdown20200405081101/

Jordon Armed Forces use drones to monitor curfew and curb virus spread

http://www.rfi.fr/en/wires/20200405-jordan-becomes-latest-mideast-country-deploy-drones-virus-response

Uttarakhand Information Technology Development Agency, India, deploys Mavic to assist police

https://www.devdiscourse.com/article/law-order/993624-ukhand-police-using-drones-to-successfully-implement-lockdown

Fiji police force acquires DJI Inspire and Mavic drones to aid in COVID-19 movement monitoring

https://www.fbcnews.com.fj/news/covid-19/drones-to-help-enhance-police-monitoring-work/

Jalandhar Police, India, deploys drones at strategic locations to arrest citizens flouting curfew

www.punjabtribune.com/news/192443-jalandhar-rural-police-press-in-service-drones-to-nab-people-violating-curfew-norms.aspx

Maui, Hawaii Police utilises drones to educate, warn and arrest people violating stay home order

https://mauinow.com/2020/04/07/maui-police-will-use-drones-for-public-announcement-capabilities/

Rehoboth Beach Police complements patrols with drones to enforce emergency order

https://delawarebusinessnow.com/2020/04/rehoboth-using-drones-cameras-patrols-to-enforce-emergency-order/

Inspire 2 drone deployed in Chennai, India, for broadcasting of COVID-19 announcement

https://gulfnews.com/photos/news/drones-help-chennai-police-to-battle-covid-19-1.1586003095881?slide=4

Wing Aviation partners F&B industry for delivery of food goods amid COVID-19 pandemic

https://www.roanoke.com/news/nrv/wing-expands-drone-delivery-options-two-christiansburg-businesses-now-on-board/article_fbf00343-dc09-59fd-bf14-36a5a31e16c4.html

1.8. INFORMATIONAL (P5)

Charlottetown, USA PD add FLIR SkyRanger R70 to their operational equiptment

https://www.theguardian.pe.ca/news/local/city-of-charlottetown-purchasing-state-of-the-art-drone-for-police-force-431078/

Shirley Police, UK, to use drones to crack down on illegal motorcycle riding and nuisance

https://www.dailyecho.co.uk/news/18360168.police-fly-drones-bid-catch-bikers-causing-nuisances/

India's Railway Protection Force deploys Phantom and Mavic drones for security of railway assets

https://www.thehindu.com/news/cities/Kochi/rpf-deploys-drone-for-aerial-surveillance/article31281410.ece

Leicestershire Police deploy drones to look for missing man

https://www.leicestermercury.co.uk/news/leicester-news/drone-team-called-fears-rise-4018069

Anchorage Police used drone to find missing hiker in Alaska

https://www.accuweather.com/en/weather-news/drone-leads-police-to-lost-hiker-in-alaska-after-wind-covers-her-tracks-with-snow/714784

Nottinghamshire Police uses drone with thermal camera to find missing boy

https://www.chad.co.uk/news/people/incredible-drone-footage-shows-moment-lost-nottinghamshire-boy-was-found-2530545

Three high school student teams to collaborate and design new drone for U.S. Army

https://insideunmannedsystems.com/student-teams-picked-to-design-new-army-drone/

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.
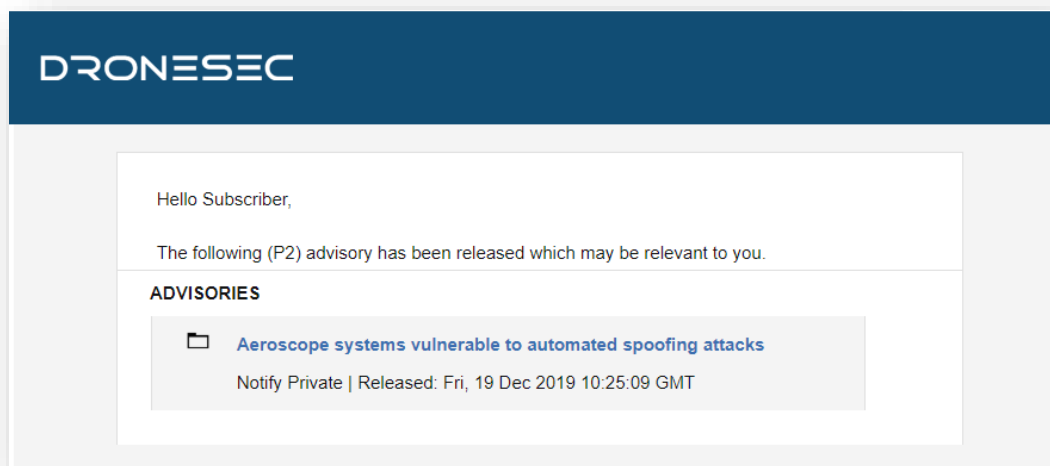

Figure 1 - A threat notification specific to a Notify customer's listed keywords.

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.