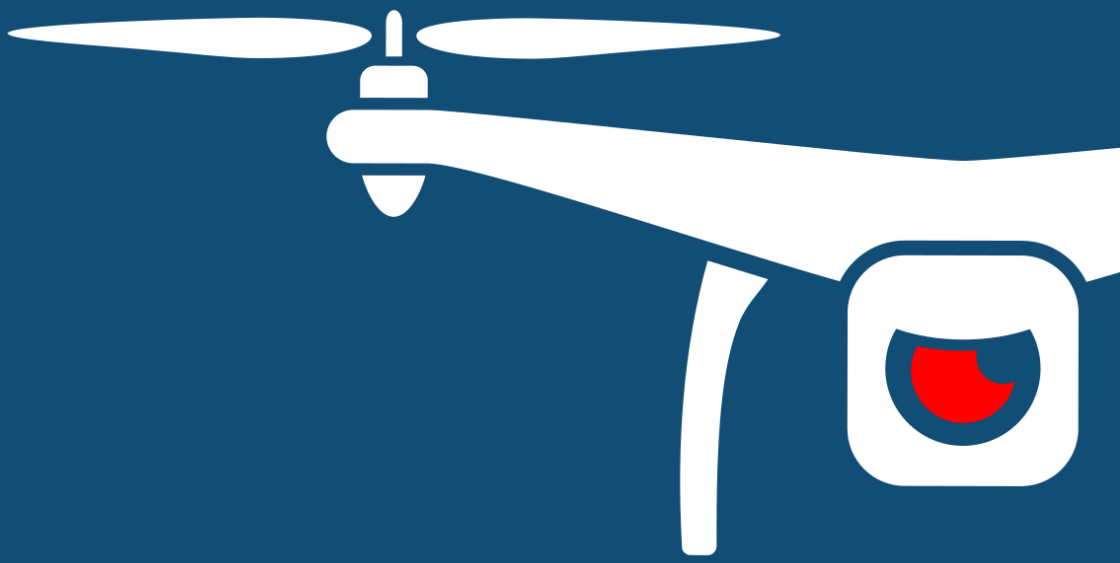
DRONE SEC
A Privasec COMPANY

NOTIFY ISSUE #5

WEEKLY THREAT INTELLIGENCE

14 January 2020 | v1.0 RELEASE



UAS HACKING, HARDENING AND DEFENCE

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

DOCUMENT **CONTROL**

PREPARATION

DroneSec (dronesec.com)

Threat Intelligence Team

Email: info@dronesec.com

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

EXECUTIVE SUMMARY

It's usually a good week when we don't push any featured advisories to Notify subscribers. Not to say it was a quiet one though – a few police incidents around the UK, India and China headline our stories for this issue.

An interesting item to come out is the NASA report on their UTM trials, in the Whitepapers and Publications section - a quality, in-depth look at future drone and UAM operations. Another fantastic read was one of their previously released reports detailing an RFC for communication security and encryption within UTM standards, linked in a previous Notify issue.

As 2020 progresses, we'll be ramping up towards our quarterly report – The State of Drone Security. This report factors in all the events, statistics and categories of incidents we've seen for the year so far, along with some analysis and case studies that have taken place since we rung in the new year.

We also have some exciting events happening in Singapore this quarter and look forward to sharing these and the results of our March training sessions with you shortly.

Of course, we continue to face a bushfire crisis in our HQ state in Victoria, Australia – it becomes very real when the threat faces our staff' friends and family. To any subscribers who may have donated to one of the many bushfire funds – thank you from all of us here at DroneSec.

- *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)

There were no featured advisories pushed to DroneSec Notify customers this week.

1.3. CYBER AND INFORMATION SECURITY (P3)

Reddit discussion on traditional Wi-Fi vs RF detection of modern COTS [1]drones

https://www.reddit.com/r/hacking/comments/efqmum/can_aircrackng_find_wireless_rc_drones_or/

US Civilian drone program to halt fleet of 1000 quadcopters over Beijing spying concerns

https://www.reuters.com/article/us-usa-drones/trump-to-halt-civilian-drone-program-over-china-tech-concerns-ft-idUSKBN1ZB0MU

1.4. NEWS AND EVENTS (P3)

Civil Aviation Authority investigates DJI Matrice as Police drone crashes

DJI's Matrice utilised by UK Police Forces were found to be falling out of the sky when coming into contact with rain or moisture. A report released by the UK Air Accidents Investigation Branch stated that the drone experienced technical failure and loss of power and control, causing the aircraft to fall vertically to the ground. This is one of sixteen incidents with a Matrice in the UK since late 2017.

https://www.thetimes.co.uk/article/police-matrice-200-surveillance-drones-affected-by-rain-hsjfdmpv0

https://www.suasnews.com/2020/01/aaib-investigation-to-dji-matrice-210-uas-registration-n-a-16-march-2019/

https://www.edp24.co.uk/news/investigation-after-norfolk-drone-destroyed-in-crash-1-6459258

Drone flies over George Pell's prison yard, forcing prisoner's transfer from jail

https://www.theguardian.com/australia-news/2020/jan/12/george-pell-reportedly-moved-to-regional-prison-after-drone-flown-over-melbourne-cbd-jail

Punjab Police struggle to combat drones flown by drug smugglers in Ferozepur

https://www.indiatoday.in/india/story/punjab-police-drone-drugs-1636555-2020-01-13

Indian bust saw drones used to carry drugs and arms consignments from Pakistan

https://www.indiatoday.in/india/story/punjab-smugglers-buying-drones-from-olx-to-fetch-drugs-arms-consignments-from-pakistan-1636261-2020-01-12

https://www.news18.com/news/india/two-chinese-drones-allegedly-used-to-smuggle-drugs-across-indo-pak-border-army-naik-among-3-arrested-2453959.html

UK Operational Police drone team publish video of FLIR-aided arrests

https://westbridgfordwire.com/police-publish-drone-video-after-first-arrests-in-keyworth/

[1] COTS – Commercial-Off-The-Shelf: Drones that can be availably purchased at a store

Turkish Police detain suspect sending drone equipment to terrorist groups in Syria

https://www.dailysabah.com/war-on-terror/2020/01/12/turkish-police-detain-suspect-trying-to-send-drone-to-al-qaida-in-syria

Drone spotted in close proximity to Medical Helicopter in Colorado, USA

https://twitter.com/COEmergency/status/1215417118616780800

China's People's Liberation Army Ground Force (PLAGF) and People's Armed Police (PAP) special forces increasingly using quadcopters and small drones for offensive operations

https://www.janes.com/article/93591/plagf-pap-special-forces-broadening-use-of-small-uavs

1.5. NEWS AND EVENTS (P4)

FAA Remote ID and COPPA law conflict, Remote ID eliminates indoor flight

https://3d.coldstreams.com/2020/01/

Reddit forum thread debates FAA Remote ID and factors on national security, hobbyists

https://www.reddit.com/r/drones/comments/ehv85g/the_proposed_rules_are_seen_as_an_important_step/

Quora thread discusses the various implications of the American Drone Security Act 2019

https://www.quora.com/What-is-the-likelihood-the-American-Security-Drone-Act-of-2019-recently-introduced-by-the-US-Senate-will-be-approved-by-Congress-and-if-it-is-how-would-it-impact-the-UAV-industry

EUROCAE forms Counter UAS working group

https://www.eurocae.net/news/posts/2019/october/new-working-group-wg-115-counter-uas-c-uas/

MI5 working with drone tech firms investigating ways to protect national security

https://standard.co.uk/news/crime/mi5-to-hire-behavioural-scientists-as-it-seeks-new-ways-to-combat-terrorists-a4332971.html

FAA gets early comments on Drone ID proposal on concerns about privacy and cost

https://www.aopa.org/news-and-media/all-news/2020/january/09/faa-gets-early-earful-on-drone-id

Sustainable Aerospace Supply Chain and Manufacturing Workshop to debate National Security

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

Altitude Angel chosen as lead UTM provider for the African Drone Forum and Lake Kivu Challenge 2020

https://www.commercialdroneprofessional.com/altitude-angel-chosen-as-lead-utm-provider-for-the-african-drone-forum-and-lake-kivu-challenge-2020/

1.6. COUNTER-DRONE SYSTEMS (P4)

Counter-Drone System launched specifically for vehicle convoys

V6000T, an advanced single-box multi-function electronic warfare (EW) system provides 360-degree gapless full dome jamming coverage in order to defeat a large number of drones from up to 2km away. It also provides protection against RCIEDs and prevent remote radio detonation of improvised explosive devices (IEDs) by jamming all-known RCIED triggering frequencies across the RF spectrum of 20-6000MHz.

https://www.unmannedsystemstechnology.com/2020/01/counter-drone-system-for-vehicle-convoys-launched/

Israel's Laser Defence System can now stop missiles, drones and mortars says Defence Ministry.

Israel Ministry of defence has revealed a technological breakthrough in the development of high-energy lasers for the interception of long-range threats in addition to their existing Iron Dome missile defence system. This all-weather technology was tested successfully and touted to be able to intercept mortar shells, drones, and anti-tank missiles with high accuracy.

https://americanmilitarynews.com/2020/01/israels-breakthrough-laser-weapon-can-now-stop-missiles-drones-and-mortars-says-defense-ministry/

FFI and KDA detect, track and shoot COTS drones at testing facility

https://www.ffi.no/aktuelt/nyheter/hvordan-stoppe-droner-som-angriper

DroneShield shares insights on adoption of Counter-UAS technology

https://blog.bisresearch.com/north-america-to-remain-the-leading-adopter-of-counter-uas-technology

WhiteFox, BlueForce and Exo-Tactik to monitor, track and analyse drones over Montreal airport

https://www.unmannedairspace.info/latest-news-and-information/whitefox-blueforce-and-exo-tactik-launch-year-long-drone-security-trial-at-montreal-airport/

Saudi Arabian Military Industries (SAMI) to deploy 'National' Counter-Drone system

https://www.defensenews.com/unmanned/2020/01/08/saudi-arabia-is-developing-a-new-counter-drone-system/

Japan to employ drone detection and counter-measure systems for 2020 Olympic Games

https://www.sfchronicle.com/news/article/Tokyo-police-add-drone-detectors-to-14958958.php

LiteEye systems join authorities in Colorado, USA 'drone mystery'

https://liteye.com/state-tests-drone-amid-mysterious-eastern-plains-drone-investigation/

1.7. WHITEPAPERS AND PUBLICATIONS (P4)

Security aspects of UTM system revealed in NASA UTM Technical Capability Level 4 report

https://utm.arc.nasa.gov/docs/2020-Rios_TM_220462-USS-Net-Perf.pdf

Defence Safety Aviation Authority publishes manual on drones

https://www.defence.gov.au/DASP/Docs/Media/Drone-Military.pdf

Global Drone Outlook 2020: Security core focus of the agenda

https://www.droneii.com/global-drone-outlook-2020#1525106654181-a2b63cd6-e0c3

Cryptographic Security of Autonomous and Unmanned Devices – Norwegian Defence Research

https://www.ffi.no/publikasjoner/arkiv/kryptografisk-sikring-av-autonome-og-ubemannede-enheter-eksisterende-forskning

https://publications.ffi.no/nb/item/asset/dspace:6444/19-02042.pdf (PDF Download - non english)

Micro-UAV Detection and Classification from RF Fingerprints Using Machine Learning Techniques

https://www.mendeley.com/catalogue/microuav-detection-classification-rf-fingerprints-using-machine-learning-techniques/ (Contact DroneSec for PDF)

1.8. DRONE TECHNOLOGY (P5)

Fully autonomous drone increases infrastructure security

Azur Drone has been developing their latest 100% automated drone solution, Skeyetech, for surveillance and security. Without any human intervention necessary, the drone is still able to carry out safe and effective operations such as automatic take off, navigation, and landing powered by Azur's proprietary artificial intelligence software. These drones can follow automatically pre-planned flight missions or have the security team give orders to the drone directly through the video management system. Skeyetech is the first all-weather European drone approved by authorities for autonomous operation.

https://i-hls.com/archives/98088

Uber and Hyundai to establish a Drone Taxi System

At the Consumer Electronics Show (CES) in Las Vegas last week, Hyundai revealed their partnership with Uber on the concept of Urban Air Mobility (UAM). Featuring a 'hub' structure to support these electric vertical take-off and landing (eVTOL) flying taxis, the service is also extended for deliveries, mobile restaurants and medical clinics. In this partnership, Hyundai will produce and deploy the air vehicles, and Uber will provide airspace support services, connections to ground transportation, and customer interfaces through an aerial rideshare network.

https://www.uasvision.com/2020/01/08/hyundai-and-uber-announce-aerial-ridesharing-partnership/

MQ-9 demos maritime surveillance and detect and avoid capabilities

General Atomics Aeronautical Systems conducted "Detect and Avoid" (DAA) system demonstrations on its MQ-9 Guardian UAV for traffic deconfliction in civil airspace. The DAA system consists of air to air radar integrated with Traffic Alert and Collision Avoidance System, and Automatic Dependent Surveillance-Broadcast. The DAA system enables safe flight of an MQ-9 in civil airspace, enhancing the integration of unmanned and manned systems in the future.

https://www.uasvision.com/2020/01/08/mq-9-demos-maritime-surveillance-and-detect-and-avoid-capabilities/

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.

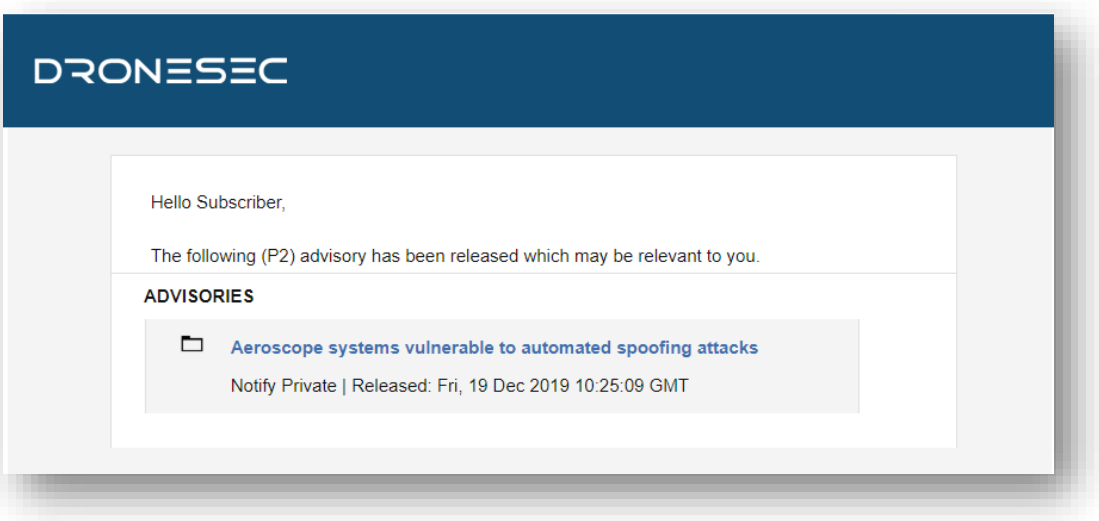


Figure 1 - A threat notification specific to a Notify customer's listed keywords.

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[2], UAV[3], RPAS[4]… • 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

[2] UAS: Unmanned Aerial System
[3] UAV: Unmanned Aerial Vehicle
[4] RPAS: Remotely Piloted Aerial System

	• Detect and/or respond to drones • Be standalone, hand-held, static or integrated with a UTM[5] or PSIM[6] 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[7], exploits or zero-days[8]. 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

[5] UTM – Universal Traffic Management System
[6] PSIM – Physical Security Information Management System
[7] OSINT: Open-Source Intelligence from the public domain.
[8] 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.