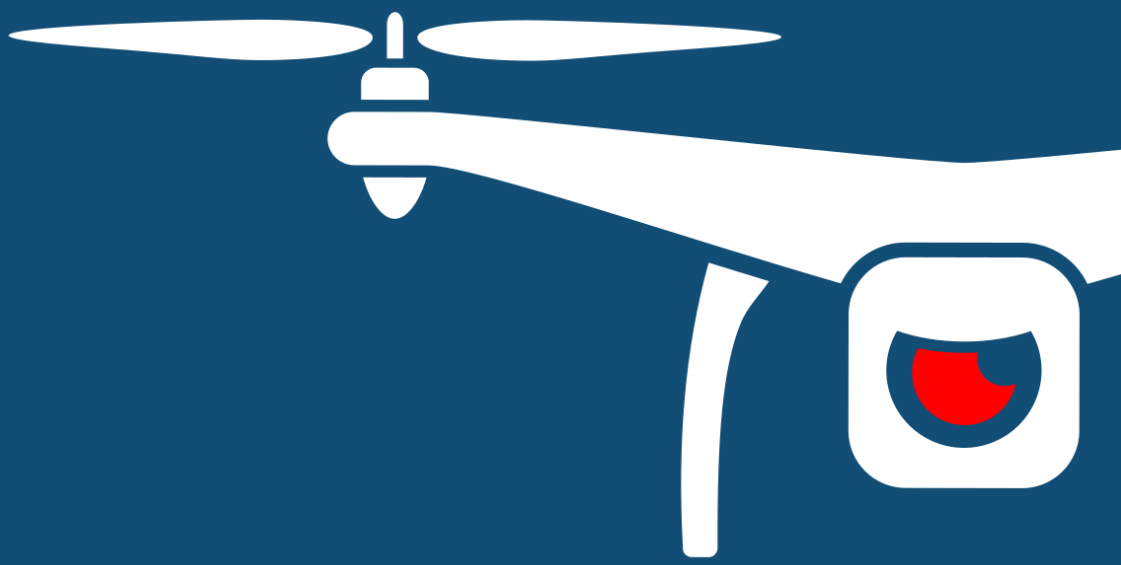
DRONE SEC
A Privasec COMPANY

NOTIFY ISSUE #63 (PUBLIC)

WEEKLY THREAT INTELLIGENCE

24 February 2021 | v1.0 RELEASE



UAS HACKING, HARDENING AND DEFENCE

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

DOCUMENT **CONTROL**

PREPARATION

DroneSec (dronesec.com)

Threat Intelligence Team

Email: info@dronesec.com

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

EXECUTIVE **SUMMARY**

Why am I receiving this report later than usual?

DroneSec has made Notify PRIVATE available to all subscribers for a subscription fee of $99 AUD per year. PRIVATE, along with being released earlier, contains the following benefits and can be purchased below:

A 'light' threat intel subscription for customers who want the latest UAV threat intel weekly newsletter without having to be a Notify Platform user. It also includes the following:

- Receive PRIVATE issues up to two days earlier than PUBLIC issues
- Access to featured reports and analysis by our UAV Threat Intel Analysts
- Access to Monthly Roll-Up's with data-driven statistics and trends
- Access to the DroneSec State of Drone Security Report
- Exclusive discounts on Training courses and Software

SUBSCRIBE TO NOTIFY PRIVATE HERE

As expected with IDEX this week, the Counter-Drone news artefacts are plenty. Of note, two key CUAS news items this week include a Black Sage tech being used by a Middle East civil defense authority successfully mitigated a drone incident at a major public event. No details have been made public yet if the drone was simply infringing within the area of malicious. In Myanmar, the coup has led to Singapore-based CUAS vendor TRD cancelling its contact with the airport and refusing to sell further systems to the country's military.

An interesting risk consideration has been highlighted with a recent UK investigation into an M300 drone crash due to its parachute system. Post-analysis, the operator identified that wind-speed and direction may provide greater understanding of drift potential in the case of parachute deployment of a drone – highlighting traditional weight scenarios may differ once safety equipment has been attached.

In a commentary piece from Germany, the Berlin Justice Department claims little drone infringements have occurred and that geo-fencing is the potential solution for future incursions, begging a variety of questions from those who understand the limitations of software-based geo-zones.

Incident reports from this week include a camouflaged DJI Phantom drone carrying narcotics that crash landed on a shop roof, and a report from NZ regarding a drone operator who's system collided with a hang glider within a manned aircraft activity zone. India suggests a series of 'sticky-bomb' IED's paired with magnets were dropped by drones in order to latch onto vehicles, with intent to cause harm.

All of these incidents and more in today's report.

As always, if you have comments or feedback, want to join in the discussion in our slack discussion group, or find the system that captures this information please don't hesitate to contact us.

- *Mike Monnik, DroneSec CTO*

TABLE OF **CONTENTS**

1. THREAT INTELLIGENCE

1.1. INTRODUCTION

Threat Intelligence to the DroneSec team means cutting-edge information, news, resources and threats delivered in a succinct and actionable way. Notify is just that – key information that can be used to prepare, prevent and identify threats and challenges which seek to take advantage of the drone industry. Our aim is to allow organisations to make more informed decisions, respond effectively and get a birds-eye view of our core focus: Drones, Counter-Drone and Universal Traffic Management (UTM) Systems – also referred to as **DCU**.

When it comes to proactively seeking out the best solutions, developing response capabilities or building resilience into your drone operations, relevant information is king. We're dedicated to ensuring you stay up to date through Notify, while getting the specific details around techniques, vulnerabilities, targets and malicious actors. Furthermore, we've made all Notify information both scalable and easily categorised, providing a mechanism for easy search but also extraction of statistics and use cases for stakeholders who need pre-mitigation insights and strategies.

For technical operators, we've included the ability to be able to prioritise relevance over noise and communicate with each other to exchange ideas and collaborate on threats. This exchange happens on a number of levels, from our slack channel, to sharing DroneSec case-studies within the platform and hearing from our partners (individuals, technology vendors, law enforcement and regulatory bodies) who supply valuable information to Notify.

Weekly reports are just that – the lifespan only covers one week of intelligence and where this might extend is when we detected or were alerted to it later on. You can rely on this information not being too old or outdated; but you're always able to browse the archives and library for older artefacts. Anything breaking news, we send off immediately to our Notify subscribers – outside of this, the report covers the rest on a weekly basis.

So how does it all work? To view our methodology, sources and scoring matrix, head down to the appendices to get a feel for it all. Otherwise, information we deem as being 'key' is featured with insights and analysis supplied for reader's benefit. The rest of the information we pick up that can be categorised as security-based intelligence for DCU is placed thereafter. Our categorisation and tagging system mean that on a monthly basis, you'll get an overview of the statistics we've seen – updated in real-time, week-on-week for pattern recognition analysis.

Something we missed? Keen to become a supplier? Want to join the Notify platform? Shoot us a message at info@dronesec.com. Otherwise, feel free to hop into the slack channel and introduce yourself: DroneSec Slack Channel. If you missed the previous issue, please email us.

1.2. FEATURED ADVISORIES

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

Intrusion and Trespass	Priority
DJI Phantom 3 found crashed on a rooftop in San Ysidro with narcotics attached	P2

Figure 1 - Featured reports and incidents are only available to PRIVATE subscribers.

Safety	Priority
Man convicted and fined $1,000 for crashing drone into paraglider, New Zealand	P2

Figure 2 - Featured reports and incidents are only available to PRIVATE subscribers.

1.3. NEWS AND EVENTS (P3)

M300 drone crash was due to excessive vibration of parachute system not securely attached

https://www.gov.uk/aaib-reports/aaib-investigation-to-dji-matrice-200-v1-uas-registration-n-slash-a-210919

Pakistan 'sticky bomb' magnet-IEDs seized by Indian police potentially dropped via drone

https://www.dailyexcelsior.com/ieds-seized-at-samba-were-magnet-fitted-dropped-at-ib-with-drone/

Black Sage reports detecting and mitigating intruding drone during public event in Middle East

https://blacksagetech.com/repository/black-sage-solution-neutralizes-drone-threat-in-middle-east

Drone spotted twice flying over school in Canada activates schoolyard lockdown measures

https://london.ctvnews.ca/drone-spotted-over-strathroy-ont-schoolyard-twice-1.5320871

UK AAIB reports Alauda Airspeeder drone crash from 8,000ft was due to poor build quality

https://www.gov.uk/government/news/aaib-report-alauda-airspeeder-mk-ii-loss-of-control-resulting-in-a-fly-away-and-eventual-crash

https://www.theregister.com/2021/02/19/airspeeder_alauda_drone_investigation_with_photos/

Taiwan's Teng Yun military drone crashes in forest due to control system malfunction

https://focustaiwan.tw/society/202102180023

Counter drone firm, TRD, cancels deal with Myanmar's Yangon Airport after military coup

https://www.todayonline.com/singapore/singapore-anti-drone-firm-cuts-myanmar-ties-after-coup

1.4. SOCIALS (P3)

Russia releases video showing soldiers training to shoot down small with rifles

https://www.instagram.com/p/CLW5XhsnaiJ/?igshid=10dy3sacm0ozt

Swarms of Mass Destruction: Are Drone Swarms Weapons of Mass Destruction?

https://www.start.umd.edu/swarms-mass-destruction-are-drone-swarms-weapons-mass-destruction

National Army announces the downing of two Houthi drones, Marib Yemen

https://twitter.com/Alhadath_Ymn/status/1363214032593956865

1.5. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P3)

Italy CAA, ENAC, issues new drone regulations compliant with new EU rules

https://www.unmannedairspace.info/latest-news-and-information/italys-enac-re-writes-national-drone-laws-to-comply-with-new-eu-rules/

AAIB issues 15 safety recommendations for UK CAA from Airspeeder drone crash incident

https://www.urbanairmobilitynews.com/emerging-regulations/uk-airspeeder-drone-crash-report-has-wide-implications-for-operators-regulators/

UK consortium to define operating standards for routine drone operations in healthcare sector

https://www.unmannedairspace.info/latest-news-and-information/uk-consortium-to-define-operating-standards-for-routine-drone-operations-in-the-healthcare-sector/

USA FAA opens application seeking for test administrators for drone pilot safety test

https://www.faa.gov/news/updates/?newsId=96839

SESAR researches technologies to protect airports from drone incursions

https://www.sesarju.eu/news/sesar-researches-technologies-protect-airports-drone-incursions

EASA to study vulnerability of manned aircraft to drone strikes

https://www.easa.europa.eu/research-projects/vulnerability-manned-aircraft-drone-strikes

Uncertainty around brand-new drone policies a key challenge for drone operators (commentary)

https://dronestoday.org/blog/uncertainty-around-new-drone-rules-a-key-challenge-for-operators-icao-webinar/

Drone attacks on Saudi Arabia from Iraq are a new threat (commentary)

https://www.jpost.com/middle-east/drone-attacks-on-saudi-arabia-from-iraq-are-a-new-threat-659607

Non-State Actors with Drone Capabilities (publication)

https://www.newamerica.org/international-security/reports/world-drones/non-state-actors-with-drone-capabilities/

Counter drone tactics: Which drones are a real threat, and which aren't? (commentary)

https://www.ifsecglobal.com/drones/counter-drone-tactics-which-drones-are-a-real-threat-and-which-arent/

Berlin Justice Dept looks to geo-fencing for prisons against drone incursions (commentary)

https://www.world-today-news.com/high-tech-drug-pacts-by-airmail-berlin-wants-to-protect-prisons-against-drones-berlin/

A Swarm of drones – the modern artillery in the Aegean (commentary)

https://greekcitytimes.com/2021/02/21/swarm-of-drones-aegean-2/

A comprehensive walkthrough of C-UAS analysis (commentary)

https://www.forensicfocus.com/articles/a-comprehensive-walkthrough-of-counter-uav-analysis/

1.6. COUNTER-DRONE SYSTEMS (P4)

US Special Forces to soon operate hand-launched signal-jamming drones, capable of CUAS

https://www.thedefensepost.com/2021/02/23/us-special-forces-signal-jamming-drones/

US Customs and Border Patrol issues RFI on technological capabilities of counter drone systems

https://www.unmannedairspace.info/counter-uas-systems-tenders/us-border-patrol-issues-rfi-for-nationwide-c-uas-concept-whitepaper/

https://beta.sam.gov/opp/e2da5d5130b44606821ff7dd83b2f9b0/view?keywords=CBP_C-UAS_RFI

CERBAIR develops algorithm to reduce false positive drone detection in RF-heavy environments

https://euro-sd.com/2021/02/headline/21463/cerbair-counter-uav-solutions/

Numerica reveals Spyglass, a 3D short range radar for counter drone systems

https://www.numerica.us/numerica-announces-spyglass-a-new-3d-radar-for-c-uas-short-range-defense-missions/

DroneShield signs agreement with US Department of Homeland Security

https://themarketherald.com.au/droneshield-asxdro-signs-agreement-with-u-s-department-of-homeland-security-2021-02-24/

Rosoboronexport to demonstrate new counter drone system at IDEX 2021 in UAE

http://roe.ru/eng/press-service/press-releases/rosoboronexport-to-present-a-new-integrated-counter-uav-system-at-idex-2021/

MBDA launches Sky Warden counter drone system with hard and soft kill options

https://www.mbda-systems.com/press-releases/mbda-launches-sky-warden-c-uas-system/

SIGN4L introduces counter drone jammers V-Protect and NavControl-G during IDEX 2021

https://www.unmannedairspace.info/counter-uas-systems-and-policies/idex-2021-sign4l-introduces-new-counter-drone-technology-for-fixed-or-mobile-applications/

Liteye Systems launches full suite counter drone solution, Liteye Shield, with AI capabilities

https://liteye.com/liteye-systems-launches-liteye-shield-the-next-generation-of-counter-uas-defense/

Elettronica showcases ADRIAN drone detection system with four different sensors onboard

https://www.unmannedairspace.info/counter-uas-systems-and-policies/idex-2021-elettronica-exhibits-drone-interception-and-neutralisation-solution-adrian/

Kaspersky Antidrone tested in action at the Chelyabinsk Pipe-Rolling Plant

https://www.steelland.ru/news/business/12197.html

1.7. INFORMATIONAL (P4)

Embry-Riddle Aeronautical University receives grant from FAA to assure drone safety

https://news.erau.edu/headlines/eagle-researchers-receive-faa-grants-to-assure-drone-safety

French Navy selects Airbus' electrically powered Aliaca drone for maritime operations

https://insideunmannedsystems.com/airbus-aliaca-drone-chosen-for-french-navy/

Drone deployed in Dearborn County to search for missing man

https://www.fox19.com/2021/02/20/crews-search-missing-dearborn-county-man/

Netherlands border patrol to use thermal drones to fight human trafficking

https://www.dutchnews.nl/news/2021/02/drones-to-be-used-to-combat-people-smuggling/

1.8. UTM SYSTEMS (P5)

The idea that 5G can enable BVLOS missions is something of a myth (commentary)

https://www.unmannedairspace.info/utm-industry-leader-interview/the-idea-that-5g-can-enable-bvlos-missions-is-something-of-a-myth-gokul-srinivasan/

1.9. DRONE TECHNOLOGY (P5)

Drones set to benefit from enhanced satellite surveillance with pinpoint accuracy

https://www.vodafone.com/news/press-release/vodafone-tests-new-tech-can-track-vehicles-drones-and-precious-cargo-remotely-within

InfiniDome completes flight trials with Counter-GNSS jamming scenarios with GPSdome

https://www.geospatialworld.net/news/infinidome-successfully-completes-gps-jammed-scenario-flight-ops/

Iris Automation's Detect and Avoid capability integrated into Avidrone's tandem-rotor drone

https://www.irisonboard.com/avidrone-aerospace-exhibits-drone-with-iris-automation-at-idex-2021/

Poland arms their military with Warmate suicide drones from WB Electronics

https://www.defence24.pl/warmate-oficjalnie-w-sluzbie-news-defence24pl

Paramount Group unveils long range drone swarm N-Raven at IDEX 2021

http://www.paramountgroup.com/media/news/paramount-group-launches-long-range-swarming-uav-system/

Carlo Ratti Associati and Flyfire design Drone Blanket capable of simultaneous charging of drones

https://newatlas.com/drones/flying-drone-blanket-charge-launch-quadcopter-swarms/

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.

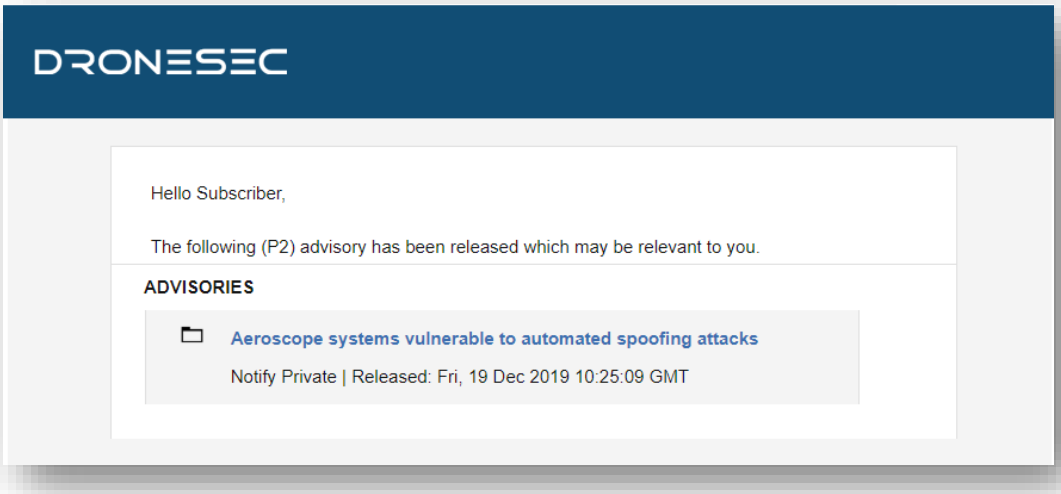


Figure 3 - A threat notification specific to a Notify customer's listed keywords.

DroneSec uses a methodology to rank, prioritise and filter intelligence pieces. This rating merges threat intelligence standards with the type of source (public, private, underground) and affected system (DCU).

Threat notifications are prioritised based on the following table:

Priority Level	Description
P1	Directly specific to a Notify customer
P2	High importance incident or situation
P3	Medium importance event or information
P4	Low interest or general news/media
P5	No direct evidence, market trends or informational

In general, (P1) alerts will only be visible to the affected customer to protect their privacy and general information security. However, abstract (P1) information will at times be shared with other Notify customers. Priority levels are often highly contentious as it requires understanding of a customer's environment, context and what might be deemed 'actionable' for them. The added spanner in the works is that DCU is made up of cyber-physical systems – there are traditional security vulnerabilities, physical and kinetic risks and even privacy, regulatory and aviation considerations in play. As a result, we set the priority level based on a number of key metrics that are very specific to our Notify customers; the more information provided about an entity, the higher the quality-gate of prioritisation we apply to our filter process.

Associated with each artefact of intelligence, you'll find a set of tags. These tags are used for indexing, searching and quickly visualising if the information is relevant to your organisation. As with any system, ours will continue to better itself as it learns more about the various artefacts that are most important to our customers, and their types of environments and systems. You'll find the tags, and examples of them, in the tables below.

There are three categories we focus on. We do not extend past these, as to keep our intelligence relevant and brief.

Tag - Categories	Description
Drones	Custom-made or Commercial-Off-The-Shelf (COTS) systems that might: • Be known as UAS[1], UAV[2], RPAS[3]… • Weigh 50g all the way to 250kgs • Are automated or manually piloted • Have associated devices, software or infrastructure
CUAS	Counter-UAS systems that might: • Be known as Counter-Drone or C-UAV

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

	• Detect and/or respond to drones • Be standalone, hand-held, static or integrated with a UTM[4] or PSIM[5] system • Have associated systems, software, infrastructure and communication protocols
UTM	Universal Traffic Management system that might: • Be known as Urban Air Mobility (UAM) or fleet management systems • Manage, track, communicate with or interdict drones and/or drone swarms • Be software and/or hardware based • Have associated systems, software, infrastructure and communication protocols

Within DCU, there are many areas of concern. For those in a position of ingesting Threat Intelligence, these are the key concerns we have determined are relevant for the information we collect.

Tag – Areas of Concern	Description
Cyber Security	Technical attack vectors, risks, threats, vulnerabilities, guides, OSINT[6], exploits or zero-days[7]. This may also contain confidentiality, Privacy, Integrity and data sovereignty artefacts
Safety	Safety concerns related to assets, environments, persons or critical systems as a direct result of the artefact. This can be caused by physical, kinetic or electronic sources.
Regulatory	Global or national law or regulatory-based amendments, announcements or ordinance that affect DCU.

Sometimes the artefacts may cover a range of sectors. For organisations looking to filter out noise, this is a key tag that will help provide insight into their chosen sectors.

Tag – Affected Sector	Description
Residential	Houses, suburban areas and private property.
Commercial	Cities, major working areas and buildings

[4] UTM – Universal Traffic Management System
[5] PSIM – Physical Security Information Management System
[6] OSINT: Open-Source Intelligence from the public domain.
[7] Zero-day: Otherwise known as an 0day or unknown, unpatched vulnerability of which the vendor does not yet know exists.

Government	Government-managed locations
Critical Infrastructure & Security	Water, energy, docks, airports, prisons, transport, stadiums and military
All Sectors	The above sectors, combined

APPENDIX B: SOURCES & LIMITATIONS

B.1. INTELLIGENCE SOURCES

DroneSec uses a variety of government, military, law enforcement, vendor and citizen-based intelligence sources. Not all of these sources are public. Sources or artefacts that cannot be verified by a third-party are clearly marked.

Source Name	Description	Intelligence Type
International Aviation Authorities	Aviation authorities are the regulatory bodies for managing air and drone activities within a range of jurisdictions. Their level of access includes pilot, airport, airprox and public incident reports.	Statistics Incidents
Academic Sources & University Agreements	Keyword alerts on various academic portals and research agreements with Higher Education provide Notify with the latest journals and papers with a focus on DCU.	Research Papers Studies and Reports
Pilots – Commercial and Private Airlines	Pilots currently active in the commercial or private airline industry.	AirProx Reports Visual Identification Reports
Commercial Partnerships	Our partners in the military defence, commercial vendor and security industry exchange intelligence with Notify.	Statistics Incidents Sentiment and chatter Vulnerabilities and Exploits
Counter-UAS vendors	Counter-UAS vendors with multiple systems in place around the globe. Their systems detect, record and (where allowed) react to malicious drones. Detection telemetry data is shared with Notify.	API and manually provided statistics
DroneSec Research	The DroneSec team conducts penetration tests, vulnerability analysis, aerial threat simulations and forensics on a variety of DCU which results in zero-day intelligence of various systems. Whilst respecting the privacy of our clients, statistics and agreed information is shared with Notify.	Incidents Whitepapers Research Papers Vulnerabilities and Exploits Open-Source Intelligence
Deep, dark and surface web communication channels	Groups, message boards and forums dedicated to modding and bypassing common drones and counter-drone controls. DroneSec actively participate and contribute in these forums to better understand the threats and risks relevant to our clients.	Manual and automated analysis based on keywords and word-clouds.
Information Security Sources	A variety of public and private sources within the Information	Vulnerabilities and Exploits Incidents

	Security, threat intelligence and Open-Source Intelligence (OSINT) communities provide Notify with recent, actionable information.	Whitepapers Research Papers Sentiment and Chatter
Newsletters and Email Lists	A variety of commercial (paid) and public sources. Gated content is exchanged with Notify within a strict agreement basis. Good examples of public sources include the Center for Study of the Drone (Bard College).	News Incidents Studies and Reports
Law Enforcement	Notify collects information from public, private and Freedom of Information (FOI) portals from Law Enforcement and shares combined metrics back to agencies.	Events Incidents Statistics
Proprietary aggregation software - Search Engines - Social Media - Government Sources	The DroneSec Notify secret sauce. Our aggregators, dorks, scripts and macros receive, filter and analyse DCU-related data, filtering for relevant and actionable information.	News Events Incidents Whitepapers Research Papers Sentiment and Chatter
Subscribers & Individuals	Subscribers of dronesec.xyz, dronesec.com and individual contacts provide manual reports to the Notify service. Contact us to see how exchanging Threat Intelligence could provide additional support to your organisation.	Incidents Research Papers Sentiment and Chatter

B.2. LIMITATIONS

Intelligence gathering reflects a point-in-time notification and/or analysis in-scope objectives (DCU). Future changes to the artefacts and the availability of new information could introduce retraction of statements or alter the wording, ratings and analysis of artefacts outlined within this report.

While DroneSec conducts in-depth fact-checking and evidence-based analysis of the information, sources and events, we aggregate information that may not be proven to be factual. Wherever possible, we try to mark this as such. DroneSec pushes for quality over quantity – but understands the needs for a broad approach to intelligence within DCU. Not all Notify reports will include analysis; delivery is subject to time the Intelligence is detected and its availability at time of Notify release.

Another limitation to the report is the lack of introductory material for a new reader to the DCU space. While news events, situations and analysis can help, newcomers to the industry can get in touch with us at info@dronesec.com or via the slack channel to seek additional clarification on topics, phrases or informational courses that might uplift their knowledge and understanding in the area.