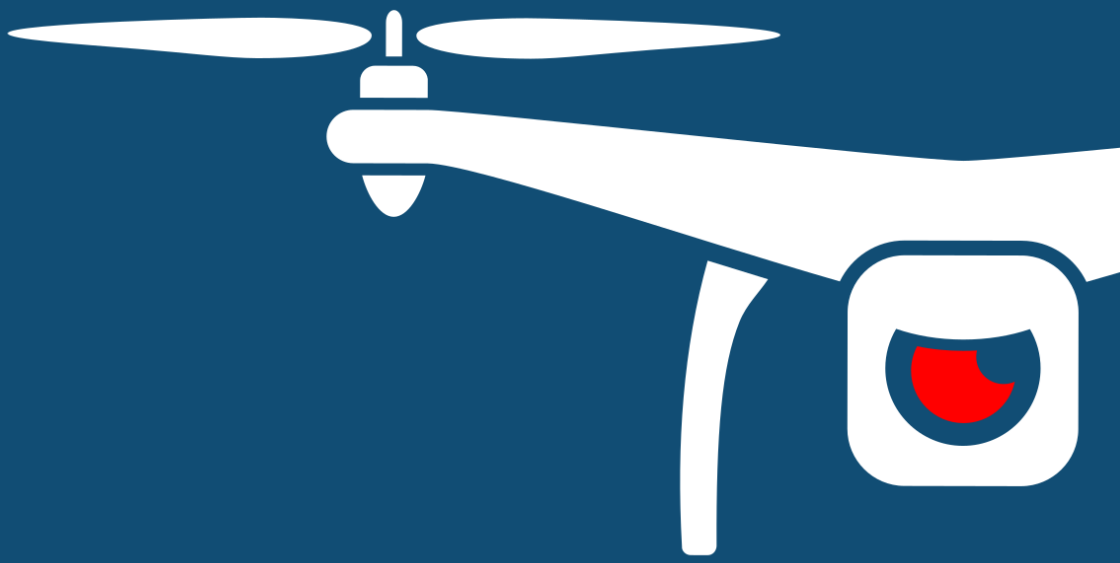
DRONE SEC
A Privasec COMPANY

NOTIFY ISSUE #37 (PUBLIC)

WEEKLY THREAT INTELLIGENCE

26 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

A whirlwind week here in Australia as we have RFI's released for both our Air Traffic Management systems by Airservices and mandatory drone registration changes by CASA. Off the back of the Flight Information Management System (FIMS) and the article on ATM Cybersecurity Challenges, we continue to search for effective frameworks for transitioning security learnings from both the cyber-security and aviation industry into UAM that includes drone systems.

In the middle east, Turkish drones continue to dominate the conversation, although an IDF-controlled DJI Mavic 2 was downed and recovered by Hezbollah. The IDF have confirmed the incident and suggested that data leakage is not a concern – this is an interesting take on the situation, and we will be listening for any chatter to suggest otherwise.

UAV Threat Intelligence continues to play a role in the India-Pakistan border wars, with India's intelligence wing confirming intel has pointed to incoming threat actors and nefarious use of equipment in the coming weeks. A common discussion point a few years ago was an article called "Who's selling drones to terrorist groups?" for which the team often surmised if purchase details by military and non-state actors could feed into threat intelligence about future adversarial use of UAS.

It's become something of a regularity to observe UAS incidents around prisons in Canada. Unlike most national trials where drone detection activities take place in airports, Canada is investing a sizeable amount into a drone detection programme for prisons. The data here will be extremely valuable in dissecting the trends and analysis required to question the investment and response required for individual facility needs. All this and more in today's report.

Depending on time, you may see DroneSec presenting at the IDGA Counter-UAS Summit. Are you attending? If so, we hope to see you there; quite an exciting line-up.

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
Warkworth Institution undergoes lockdown with discovery of contraband from suspected drone drop	**P2**

Summary

Warkworth Institution activated a lockdown after packages were discovered within the perimeter of the prison.

Overview

Correctional officers of Warkworth Institute, Canada, issued a lockdown for the prison when several packages were discovered on the perimeter. A drone drop was suspected and the officers carried out a search within the prison to look for unauthorised items and determine the source of the packages. No further information was released.

Analysis

Drones allow malicious users to operate safely with a low risk of being apprehended by law enforcement agencies due to them being disconnected from the threat. Drone are also easily obtainable and is a cost-effective tool, empowering such users to carry out delivery drops into restricted areas which may not have been easily committed previously.

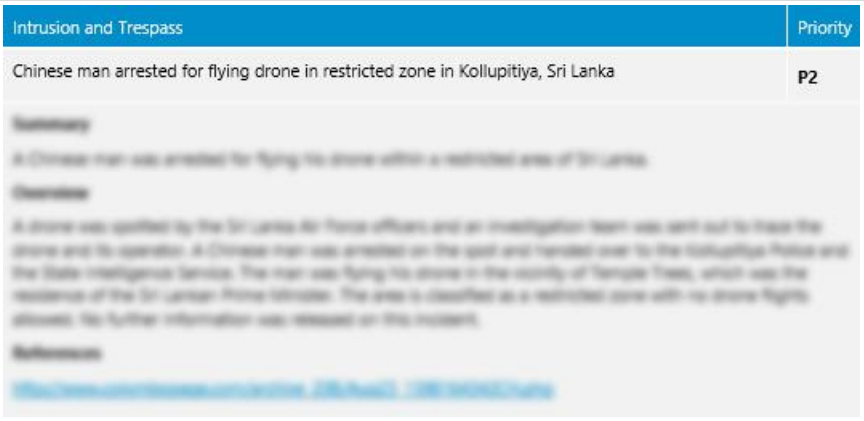
However, the risk of being traced due to visual sighting or forensics exploitation on a downed drone (via its video and photo footage) poses an exposure risk to the operators. Operators are not impervious from identification as the drone video footage and telemetry can allow law enforcement to trace the drone back to its take-off point. Facial recognition of the offenders may also be captured within the video, allowing easier investigation and apprehension of the offender.

Recommendations

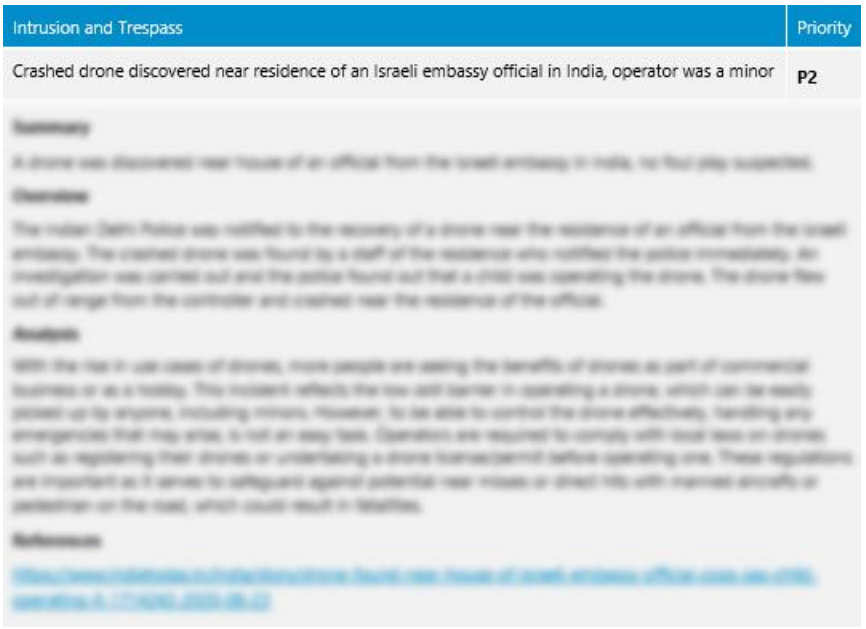
DroneSec recommends all perimeter security agencies to focus on continuous practice or tabletop exercise on the SOP for drone incursions. This practice will help to govern the process, people and methodology in handling drone intrusions such as collecting evidence, responding to potential drone threats and searching of drone operators in a pre-determined area around the prison grounds.

References

https://www.canada.ca/en/correctional-service/news/2020/08/lockdown-and-search-at-warkworth-institution.html



Intrusion and Trespass	Priority
Chinese man arrested for flying drone in restricted zone in Kollupitiya, Sri Lanka	P2



Intrusion and Trespass	Priority
Crashed drone discovered near residence of an Israeli embassy official in India, operator was a minor	P2

Interested in getting access to reports like these? Please get in contact with the DroneSec team to see what our tailored intelligence plans or platform access can provide you with info@dronesec.com

1.3. VULNERABILITIES AND CYBER SECURITY (P3)

Air Traffic Management: A Cybersecurity Challenge

https://www.asi-mag.com/air-traffic-management-a-cybersecurity-challenge/

1.4. NEWS AND EVENTS (P3)

DJI Mavic Pro operated by Israeli IDF shot down in Lebanon and recovered by Hezbollah

https://www.theyeshivaworld.com/news/headlines-breaking-stories/1894744/hezbollah-shoots-down-idf-drone-over-lebanon.html

https://twitter.com/kaisos1987/status/1297508337710440448

Bomb-laden Houthi drone shot down by Saudi-led coalition in Yemen

https://www.nytimes.com/reuters/2020/08/20/world/middleeast/20reuters-saudi-security-yemen.html

India border intelligence wing: Pakistan to drop bombs and send contraband into India via drones

https://economictimes.indiatimes.com/news/defence/pakistan-to-use-drones-to-bomb-security-establishments-near-jammu-border-bsf/articleshow/77703164.cms

Arkansas Army RQ-7 military drone loses contact and crashes during routine training, USA

https://www.nwaonline.com/news/2020/aug/25/arkansas-army-national-guard-drone-crashes-near/

Man sentenced for failed narcotics drone delivery to Lincoln Correctional Center in 2018 (Update)

https://www.usnews.com/news/best-states/nebraska/articles/2020-08-25/man-sentenced-for-using-drone-to-deliver-drugs-to-prison

1.5. SOCIALS (P3)

Turkish surveillance drone shot down by PPK in Shiladze, Iraq

https://twitter.com/BarzanSadiq/status/1296354685729767424

Turkish drones bomb the town of Sinjar in Northern Iraq

https://twitter.com/SkyNewsArabia_B/status/1298353188693778432

Turkish TB2 drones accompany 300-vehicle convoy in Libya

https://twitter.com/HasairiOuais/status/1297130622440349697?s=20

Drone industry is flying off the back of escalating global tensions (webinar)

https://stockhead.com.au/stockhead-tv/stocktalk-drone-industry-is-flying-off-the-back-of-escalating-global-tensions/

1.6. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P4)

Tanzania Civil Aviation Authority extends mandatory UAS registration to 30th Aug 2020

https://www.thecitizen.co.tz/news/Register-or-throw-away-your-drone--TCAA/1840340-5613270-dp93l6/index.html

Australian Aviation Authority release updated proposal on drone registration, seeks consultation

https://consultation.casa.gov.au/stakeholder-engagement-group/proposed-remotely-piloted-aircraft-rpa-regulatory/consult_view/

East Asia military balance at risk from new missiles and drones (commentary)

https://asia.nikkei.com/Politics/International-relations/East-Asia-military-balance-at-risk-from-new-missiles-and-drones

Drones in Northern Africa: in whose interest? (commentary)

https://dronewars.net/2020/08/25/drones-in-the-sahel-in-whose-interest/

The US Navy Plans to foil super swarm drone attacks by using the swarm's intelligence against itself (commentary)

https://www.forbes.com/sites/davidhambling/2020/08/26/how-us-navy-plans-to-foil-massive-super-swarm-drone-attacks

1.7. COUNTER-DRONE SYSTEMS (P4)

US FAA opens request to test and evaluate counter drone technologies at Atlanta airport

https://www.faa.gov/news/updates/?newsId=95737&omniRss=news_updatesAoc&cid=101_N_U

Department 13 deploys protocol manipulation MESMER counter drone system in India

https://department13.com/department-13-successfully-deploys-mesmer-c-suas-platform-to-indian-government/

US Air Force issues $90M contract to SRI for counter-drone systems and support

https://www.defensenews.com/unmanned/2020/08/25/air-force-issues-90-million-contract-for-counter-drone-systems-and-support/

Canada spends CAD$6M on drone detection programme for prisons (commentary)

https://www.blogto.com/city/2020/08/drugs-weapons-drone-ontario-prison/

Demand for drone counter-measures likely to grow (commentary)

https://dronedj.com/2020/08/24/demand-for-counter-drone-products-likely-to-grow/

1.8. UTM SYSTEMS (P4)

Airservices Australia release requirements for Flight Information Management System

https://newsroom.airservicesaustralia.com/releases/utm-commences-with-airservices-release-of-its-requirements-for-a-flight-information-management-system

https://engage.airservicesaustralia.com/fims

UAVOS reveals SumoAir, electric air taxi concept for urban transportation

https://www.uavos.com/uavos-presented-a-concept-sumoair-urban-air-taxi

Airservices Australia and QUT to develop tech for automated real time drone flight approval

https://newsroom.airservicesaustralia.com/releases/new-tech-to-open-up-skies-for-drone-operations

AutoMicroUAS and Unifly partner for BVLOS test flights in India

https://www.geospatialworld.net/news/india-embraces-bvlos-flights-together-with-unifly/

Roads Transport Authority and Dubai Air Navigation Services sign MOU for UAM development

https://www.zawya.com/mena/en/legal/story/Drones_could_have_special_air_corridors_in_Dubai-ZAWYA20200825104734/

1.9. INFORMATIONAL (P4)

US DoD: Altavian, Parrot, Skydio, Teal, and Vantage Robotics as approved drone vendors

https://www.defense.gov/Newsroom/Releases/Release/Article/2318799/defense-innovation-unit-announces-suas-product-availability-to-provide-secure-c/

US Customs and Border Patrol incorporates drones for land and sea border patrols

https://spectrumlocalnews.com/nys/jamestown/news/2020/08/20/u-s--customs---border-patrol-taking-to-the-skies-with-new-drone

Axon partners Fotokite to provide law enforcement live drone footage and aerial awareness

https://fotokite.com/axon-fotokite-to-offer-tethered-drone-technology-to-law-enforcement/

Australian pilots and contractors drafted to train and pilot UK's Reaper drone in Syria and Iraq

https://dronewars.net/2020/08/18/revealed-private-contractors-flying-british-armed-drones-as-number-of-uk-strikes-in-iraq-increase-again/

Vancouver police deployed thermal sensing drone to apprehend man hiding in water

https://www.vancouverisawesome.com/vancouver-news/vancouver-police-drone-thermal-imaging-locate-swimmer-evading-officers-video-2653555

1.10. DRONE TECHNOLOGY (P5)

US Army research energised power lines to help drones to detect and avoid collision

https://www.army-technology.com/news/us-army-power-line-sensors-small-drones/

Valqari introduces drone agnostic, fully autonomous drone delivery station

https://www.businesswire.com/news/home/20200819005087/en/

US Army awards 10 contracts on development of Air Launched Effects

https://www.army.mil/article/238438

Heron Systems AI claims victory against human fighter pilot in AlphaDogfight

https://www.thedrive.com/the-war-zone/35888/ai-claims-flawless-victory-going-undefeated-in-digital-dogfight-with-human-fighter-pilot

Singapore's National Environment Agency uses DJI Phantom 4 to check roofs for dengue sites

https://www.straitstimes.com/singapore/drones-join-nea-battle-against-dengue

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) UAS 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.

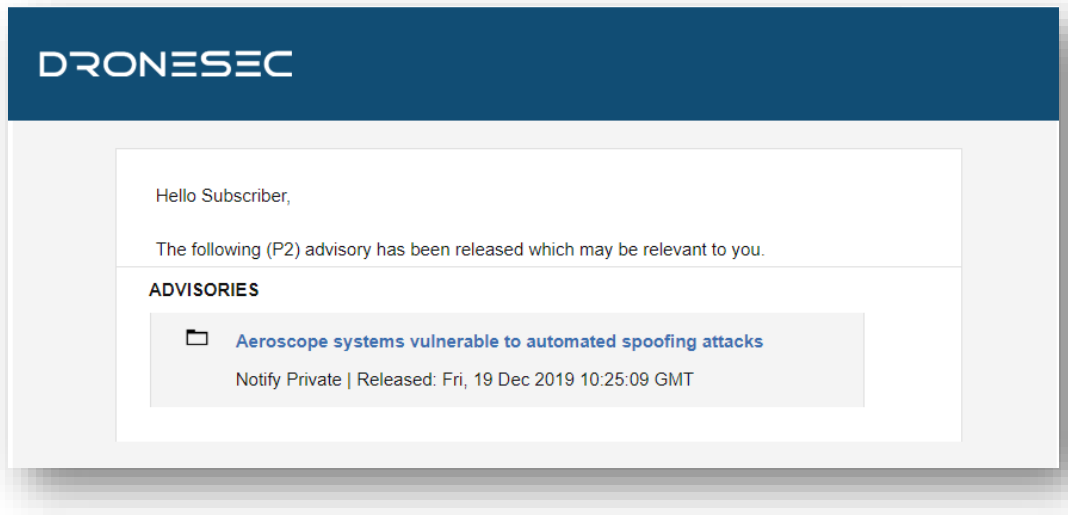


Figure 1 - A threat notification specific to a Notify customer's listed keywords.

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 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.