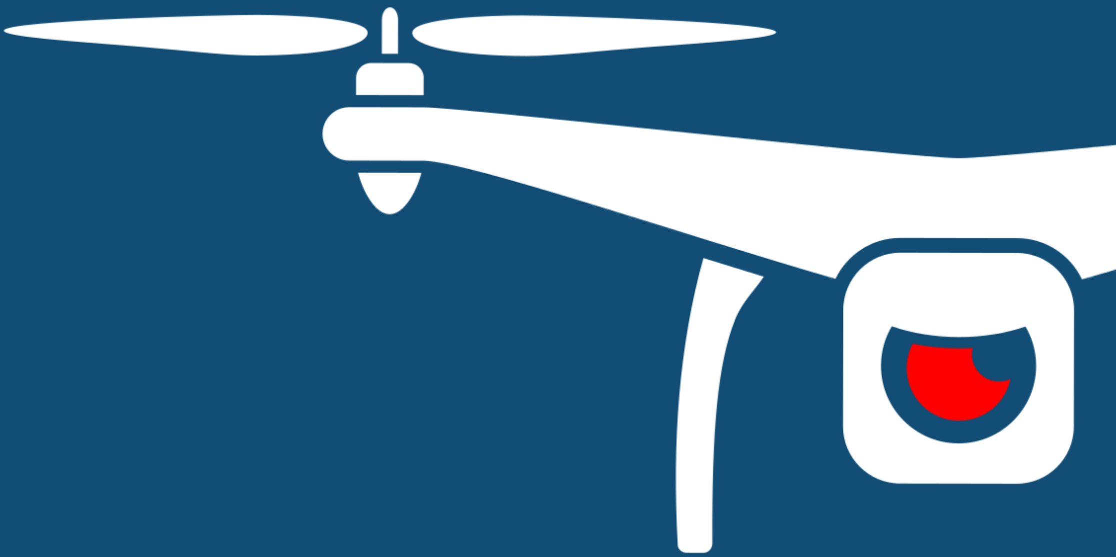
DRONE SEC

A Privasec COMPANY

NOTIFY ISSUE #45 (PUBLIC)

WEEKLY THREAT INTELLIGENCE

21 October 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

This week, we have some exciting updates to provide Notify platform users and clients. We announced a strategic partnership with DroneALERT (drone-detectives.com) to 1) enrich the global knowledge and intelligence sharing of UAV incidents, and 2) provide some level of incident case management. This means if an incident is reported, it can be overlaid with detected incidents nearby, attributed threat actors or even detect patterns within similar events. Further to this, for certain reports that are made by contributors, these will be triaged and appear within the system. This is great for a number of reasons, but we will let you get into the details yourself. The DroneALERT team are fantastic and wholly committed to our goal of focusing on rogue and malicious flights whilst protecting the innovation of hobbyists and commercial operators https://www.suasnews.com/2020/10/dronesec-and-dronealert-partner-on-threat-intelligence-sharing-and-incident-case-management/dronesec-dronealert/

The DroneSec team also expanded, adding another Drone Security Consultant in Brisbane, Australia, who joins us with over 10 years' experience as a military fighter jet pilot, with software engineering and penetration testing experience.

This week we had quite an interesting evolution come out of Liteye systems, with a CUAS modelling and simulation system. We've seen autonomous software simulations for rogue drone behaviour but never a focus on how a certain CUAS may react and simulating the effect. Moving onto law enforcement, a combination of pilot skills and usability resulted in the apprehension of a suspect with very little interaction or potential harm to operators. It is an intriguing watch and quite convincing to see the benefit of its use to first responders.

In the UK, another near-miss between a drone and passenger plane at Heathrow airport has been released by the airprox board. In Singapore, investigators used drone forensics to identify past infringements and piece together the unauthorised activities of the individual. Things continue to heat up in the Armenian-Azerbaijan conflict, where the Armenian side allege Turkish air control posts are those operating the combat UAVs – not Azerbaijan.

There was some very, very interesting information shared in podcasts this week. Popular Front cover UAS in combat over Armenia-Azerbaijan and the Inspector General the Justice Department is interviewed on the threat of surveillance and contraband from drones into its prisons. Both are very detailed and highly recommended by the team.

As always, if you have comments or feedback, want to join in the discussion in our slack group, or find out how we capture all 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.

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
Singaporean man arrested for flying without permit over restricted areas	**P2**

Summary

A Singaporean youth was arrested for flying his drone over multiple military bases and restricted areas.

Overview

An eyewitness spotted the drone flying within the aerodrome and reported the incident to the local authorities. Police arrested the youth and seized his drone thereafter. Forensics found that the youth had flown his drones on several occasions, each in restricted areas such as depots, military bases and within aerodromes. In addition, photographs of these restricted areas were also found taken by the drone. The operator did not have a valid permit and had also flown up to 543m in altitude, above the 200ft (61m) permitted height allowance for drone operations.

Analysis

Another great example of drone forensics being utilised by law enforcement to assess and provide attribution for unauthorised drone use. Forensics should not just stop at identifying illegal actions – analysts should also record and document the areas the operator chose to take-off from. Most likely, other operators will choose to launch from similar areas given the geography or characteristics of the terrain. By continually extracting these take-off areas, law enforcement can identify patterns or potential pre-text actions taken by similar malicious operators in the future.

With the rise in use cases of drones, more people are seeing the benefits of drones as part of their business activities or as a hobby. However, despite multiple public broadcasts on the rules for drone operations, there are still many users who choose to fly drones into restricted areas due to ignorance or plain disregard of aviation laws. These acts have a negative effect on the drone industry and may see regulators enforcing more stringent rules affecting the legitimate and commercial drone operators more than the intended offenders.

Recommendations

Drone operators must be cognisant of the laws set in place by their country. Singapore has experienced stiffer penalties being passed to clamp down on errant drone users.

While it may not be possible yet to provide city-wide coverage of drone detection and counter-drone systems, basic preparation measure can be set in place to respond to such incidents. A drone management plan and Standard Operating Procedure (SOP) should be drafted to govern the methodology in handling rogue drones. Enforcement agencies can also appeal to the help of the public as an eyewitness; it is beneficial to have a process for such evidence, and then carefully curated for collection and logging.

Organisations should also aim to undertake mock simulations to hone their response, improve communication flow between involved agencies and practice logging and monitoring of repeated cases. This practice can aid agencies in responding during time critical scenarios, mitigate inherent risks and surface challenges in communication and regulatory requirements.

References

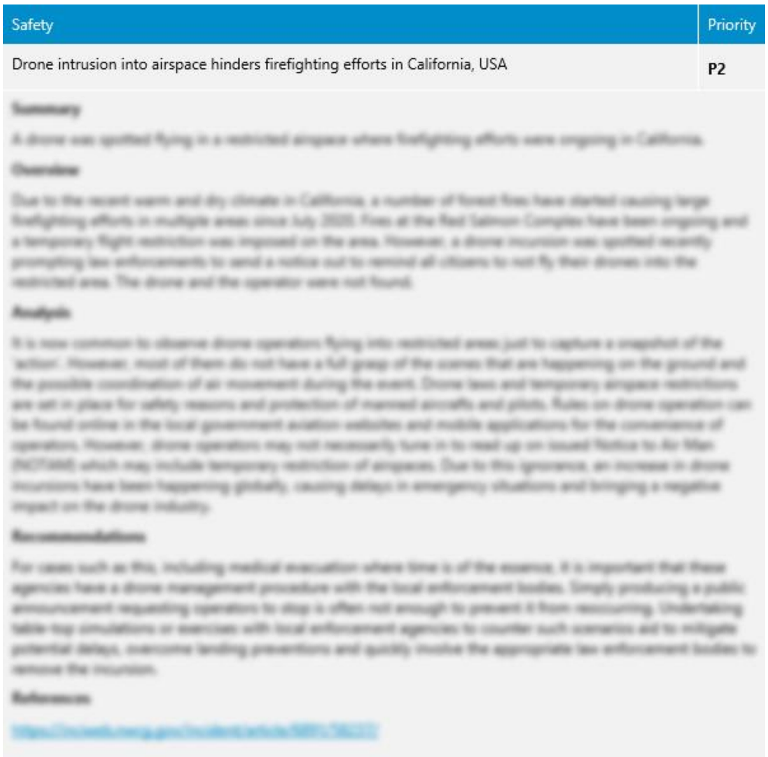
https://www.straitstimes.com/singapore/courts-crime/youth-allegedly-operated-drone-over-no-fly-zones-including-mindef-gombak-base

https://www.channelnewsasia.com/news/singapore/man-charged-drone-mindef-gombak-base-gali-batu-depot-13285208

Safety	Priority
Saudi Airlines passenger plane had near miss with drone at Heathrow Airport, United Kingdom	**P2**

[illegible]

Figure 1 - *Can't see these articles? Unlock the full analysis by getting in touch with us info@dronesec.com*



Safety	Priority
Drone intrusion into airspace hinders firefighting efforts in California, USA	**P2**

[illegible]

1.3. NEWS AND EVENTS (P3)

Atlanta PD publishes drone video on arrest of murder suspect with minimal risk to officers

https://dronedj.com/2020/10/17/atlanta-police-drone-arrest/

The Indian Army is training soldiers to take down drones due to increasing drone threats

https://www.dnaindia.com/india/report-indian-army-is-training-soldiers-to-kills-drones-here-s-why-2849744

Pilot trainee flew around drone to avoid mid-air collision, Perthsire, United Kingdom

https://www.thecourier.co.uk/fp/news/local/perth-kinross/1658731/flying-student-avoids-high-risk-of-collision-with-drone-in-perthshire/

Killaloe Police, Canada front complaints of multiple flights over residential homes

https://www.kingstonthisweek.com/news/local-news/killaloe-opp-remind-drone-operators-about-the-rules-after-complaint-of-flights-over-residential-areas/wcm/26fe5548-f8f8-4cbf-86f3-8f60ed9973a2

Precise Turkish and Israeli-made drone strikes by Azerbaijani destroy Armenian artillery guns

https://www.france24.com/en/live-news/20201017-azerbaijani-drone-strikes-pick-off-karabakh-artillery

Armenia shoots down Turkish-made Bayraktar TB2 drone in war against Azerbaijan

https://massispost.com/2020/10/artsakh-defense-forces-shoot-down-turkish-bayraktar-drone/

https://www.youtube.com/watch?v=Hz86Fl9jITo

Armenia claim direct involvement from Turkey: Azerbeijani UAVs are being controlled by Turkish air control posts

https://www.kommersant.ru/doc/4537733

1.4. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P4)

USA Office of Inspector General initiates audit on FAA 's oversight of CUAS technology

https://www.hstoday.us/industry/oig-plans-to-assess-faa-oversight-of-counter-drone-technology/

https://www.oig.dot.gov/sites/default/files/FAA%20cUAS%20Oversight%20Audit%20Announcement.pdf

Concerns over Chinese made drones continue as executive agencies update their drone policies

https://www.crowell.com/NewsEvents/AlertsNewsletters/all/Concerns-Over-Chinese-Made-Drones-Continue-as-Executive-Agencies-Update-their-Drone-Policies/pdf (PDF Document

How U.S. Army's billion-dollar gamble on drone defence could go wrong (commentary)

https://www.forbes.com/sites/davidhambling/2020/10/14/how-us-armys-billion-dollar-gamble-on-drone-defense-could-go-wrong/#3c3d4be25898

Tanks future on battlefields in doubt due to drones, rockets (commentary)

https://www.uav.org/tanks-future-on-battlefields-in-doubt-due-to-drones-rockets/

A partial ban on autonomous weapons would make everyone safer (commentary)

https://foreignpolicy.com/2020/10/14/ai-drones-swarms-killer-robots-partial-ban-on-autonomous-weapons-would-make-everyone-safer/

Security Drones: Welcome to the future (commentary)

https://www.sdmmag.com/articles/98678-welcome-to-the-future

Audio-Based Aircraft Detection System for Safe RPAS BVLOS Operations

https://www.preprints.org/manuscript/202010.0343/v1/download (PDF Document)

1.5. COUNTER-DRONE SYSTEMS (P4)

Fortem partners Mikuni for counter drone solutions on critical infrastructure and civilian events

https://www.globenewswire.com/news-release/2020/10/16/2109624/0/en/Fortem-Technologies-Partners-with-Mikuni-Corporation-to-Provide-Security-Solutions-Against-Drone-Incursions-for-Civilian-Events-and-Critical-Infrastructure.html

USAF seek RFI to upgrade existing CUAS weapons against growing drone threat

https://www.airforcemag.com/usaf-scoping-out-upgrades-to-counter-uas-weapons/

Joint Counter sUAS Office (JCO) set to announce CUAS requirements October 30

https://www.defensedaily.com/jco-looks-use-counter-uas-threats-hazards/unmanned-systems/

https://www.armytimes.com/digital-show-dailies/ausa/2020/10/17/with-artificial-intelligence-every-soldier-is-a-counter-drone-operator/

Liteye, Numerica and Aegis release CUAS modelling, simulation and training system

https://www.globenewswire.com/news-release/2020/10/20/2110842/0/en/Liteye-Systems-Launches-the-Virtual-Liteye-C-UAS-Counter-Unmanned-Aircraft-Systems-Simulator.html

MARSS Group introduces kinetic denial function in its CUAS systems with jamming capabilities

https://internationalsecurityjournal.com/marss-boosts-cuas-solution/

Former COO of Blackberry Cylance joins the WhiteFox board of directors

https://www.suasnews.com/2020/09/former-schneider-electric-executive-and-blackberry-cylance-president-daniel-doimo-joins-whitefox-board-of-directors/

Transportation Security Administration selects Innovation Task Force one counter-UAS system

https://www.tsa.gov/sites/default/files/itf_newsletter_4_vf.pdf (PDF Document - pg.2)

1.6. UTM SYSTEMS (P4)

The Inevitable Merge of UAM and UAV: Part 1 (commentary)

https://www.commercialuavnews.com/infrastructure/the-inevitable-merge-of-uam-and-uav-part-1

There will be a time when traditional traffic will yield to drone traffic (commentary)

https://www.unmannedairspace.info/news-first/there-will-be-a-time-when-traditional-traffic-will-yield-to-drone-traffic-faas-jay-merkle/

Purdue University deploys POLARIS system for UTM simulation

https://www.uavexpertnews.com/2020/10/purdue-university-uas-to-deploy-simlat-utm-simulation/

1.7. INFORMATIONAL (P5)

Tasmania Police awarded with AUD$400,000 four years drone program with drones and training

https://www.examiner.com.au/story/6974227/new-drones-to-help-tasmania-police-target-offenders/

Cass County deploys thermal drone to find missing elderly woman, Kansas City

https://www.kansascity.com/news/local/article246479170.html

Lethbridge police use thermal drones to search for missing man, Canada

https://lethbridgeherald.com/news/lethbridge-news/2020/10/16/police-use-drone-to-find-missing-person/

UK Army reveals 190g bug-like drone with speed of up to 80km/h for surveillance operations

https://www.telegraph.co.uk/news/2020/10/19/britain-race-technological-advantage-battlefield-says-defence/

South Korean military to acquire suicide drones and anti-jamming sensors

http://www.koreaherald.com/view.php?ud=20201019000792

DroneSec and DroneALERT partner on UAV threat intel sharing and incident case management

https://www.suasnews.com/2020/10/dronesec-and-dronealert-partner-on-threat-intelligence-sharing-and-incident-case-management/dronesec-dronealert/

1.8. DRONE TECHNOLOGY (P5)

China demonstrates launching 48 suicide swarm drones from trucks and helicopters

https://www.thedrive.com/the-war-zone/37062/china-conducts-test-of-massive-suicide-drone-swarm-launched-from-a-box-on-a-truck

US Army to trial electronic warfare jamming pods on MQ-1C drones

https://www.c4isrnet.com/show-reporter/ausa/2020/10/14/us-army-tests-jamming-pod-on-gray-eagle-drone/

Viasat and AeroVironment to develop encrypted communications for U.S. Army small drones

https://www.suasnews.com/2020/10/viasat-aerovironment-team-to-develop-enhanced-type-1-encrypted-communications-capabilities-for-u-s-army-unmanned-aircraft-systems/

US Army trials quieter drones for lower detection signature

https://www.military.com/daily-news/2020/10/19/army-field-testing-quieter-drones-avoid-enemy-detection.html

1.9. SOCIALS (P5)

Federal prisons facing threats from drones dropping contraband, surveilling facilities (podcast)

https://federalnewsnetwork.com/agency-oversight/2020/10/ig-federal-prisons-face-danger-from-drones/

The Rise and Rise of Drone Warfare – Popular Front (podcast)

https://podcasts.apple.com/gb/podcast/popular-front/id1364539980?i=1000494942391

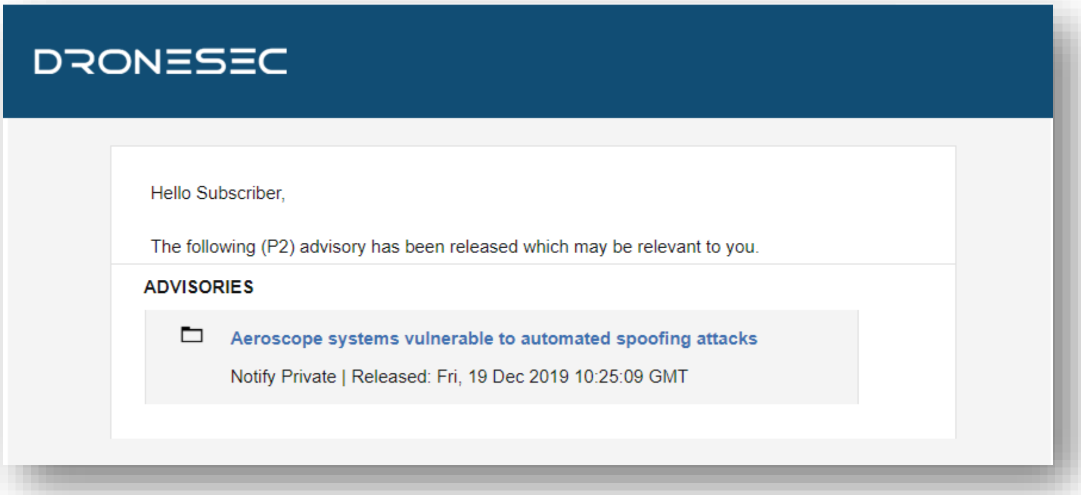
APPENDIX A: THREAT NOTIFICATION MATRIX

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.



DRONESEC

Hello Subscriber,

The following (P2) advisory has been released which may be relevant to you.

ADVISORIES

Aeroscope systems vulnerable to automated spoofing attacks

Notify Private | Released: Fri, 19 Dec 2019 10:25:09 GMT

Figure 2 - 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.