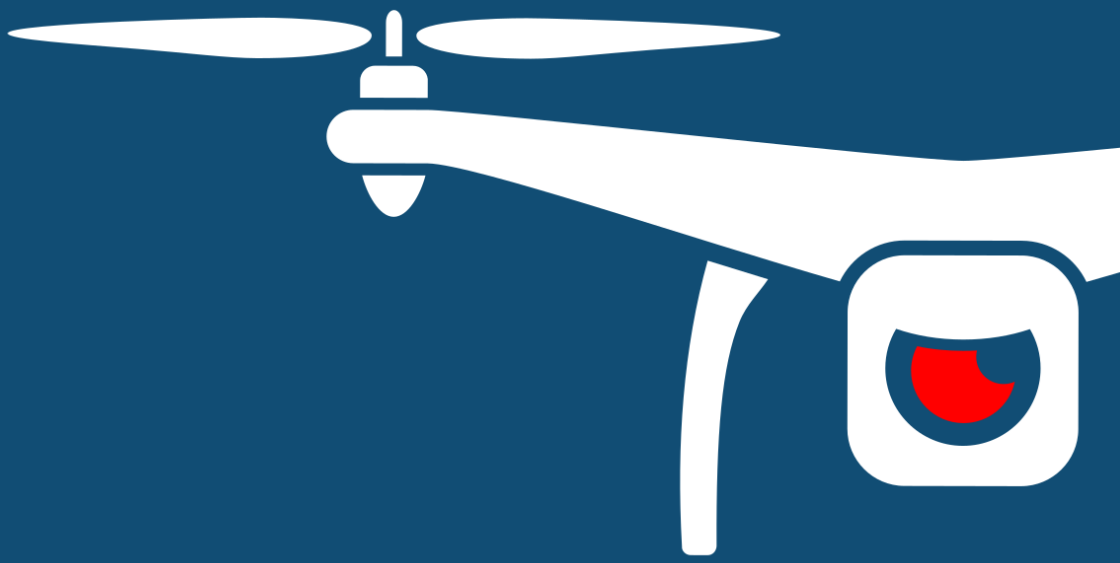
DRONE SEC
A Privasec COMPANY

NOTIFY ISSUE #31 (PUBLIC)

WEEKLY THREAT INTELLIGENCE

15 July 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

Abstract submissions close today for the World of Drones and Robotics Congress (WoDaRC) in Brisbane, QLD Australia. The DroneSec team has submitted a talk analysing a variety of drone incidents, the patterns that can be identified and the predictions that could be made from that data. We first spoke at the conference back in 2017 when we did a statistical analysis of google searches (*think "bypass NFZ", "how to fly into airports", "using a HackRF to manipulate a DJI Inspire"*) we had monitored to our then-existing drone security magazine/website, dronesec.xyz. The presentation from 2017 can be found in the Notify platform under "Knowledge Base".

A quiet week in the past 7 days with no major UAV incident headliners to be wary of; however, we continue to monitor some of the Special Monitoring Mission reports where small and long-range UAV are often the target of single and dual-GPS jamming and small-arms fire. It is indeed a warzone, but it also goes to show the tactical deployment of CUAS systems in war-time efforts and even their affect on oversight or governing bodies such as the SMM to Ukraine.

In the USA, we see the RTCA Special Committee looking to govern a sUAS detection and mitigation standard, with some work on ensuring government bodies get the tried-and-tested information from a CUAS which is advertised. The DroneSec team have a similar approach to CUAS testing and analysis which is tiered in a rating system; if you would like a copy of this document, please send us an email at info@dronesec.com or access it via the Knowledge Base section of the Notify platform.

An interesting job advertisement for the FAA has popped up, with duties including security work within Unmanned Systems while performing National Security Programs and Incident Response. Kansas University offers a Masters in IT degree with an interesting twist – a concentration on UAS security. Certainly a course to keep an eye on, and for those who are well suited in the domain and alumni of the college – it may be a great opportunity to advise or impart some of your knowledge through the board. All of the above, and more, in the below report.

An important reader request as we close off for today: we're aware of some subscribers who are not yet at the stage of requiring a fully-fledged UAV Threat Intelligence Platform but still very much miss the featured reports and articles. If this represents you, please let us know by clicking here. This way we can provide a low-cost alternative to receiving high-quality, weekly private reports without the power of the Platform's database and monitoring technology.

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.

Notice to our readers: Featured advisories have provided context and field-based learnings to important incidents within the drone ecosystem. However, with the ever-growing database that we have, DroneSec has moved onto an online repository where artefacts and reports can be tracked, classified and analysed much easier. Featured Analysis from now on are more comprehensive, wider in spectrum but only available on the Notify platform or to paid subscribers.

Intrusion and Trespass	Priority
Drone found in Indian village 15km from India-Pakistan border was from the Indian Army	**P2**

1.3. NEWS AND EVENTS (P3)

Houthi drone shot down by Yemeni Army in Al Hudaydah province, Yemen

https://www.aa.com.tr/en/middle-east/yemeni-army-downs-houthi-rebel-drone/1904255

Saudi-led coalition takes down seven explosive-laden Houthi drones and four ballistic rockets

https://www.reuters.com/article/us-saudi-security-yemen/saudi-led-coalition-intercepts-ballistic-rockets-drones-launched-by-yemens-houthis-state-news-agency-idUSKCN24D0U6

Iraqi Joint Operations Command eliminate four ISIS suicide bombers with combat drone

https://menafn.com/1100472104/5-IS-suicide-bombers-2-security-members-killed-near-Baghdad

Russia's shoots down two incoming Syrian militant drones 5km from Khmeimim airbase

https://sputniknews.com/middleeast/202007121079864937-air-defence-systems-repel-militant-drone-attacks-on-hmeimim-airbase-russian-military-says/

Azerbaijan military drone shot down during an attempted attack on the Republic of Armenia

https://en.armradio.am/2020/07/13/azerbaijan-loses-advanced-drone/

RTCA Special Committee to govern sUAS detection and mitigation standards

https://www.rtca.org/content/sc-238

Special Monitoring Mission (SMM) UAV experienced GPS signal interference in Ukraine by probable jamming near:

Avdiivka and Dokuchaievsk (long-range UAV)

https://www.osce.org/files/2020-07-10%20SMM%20Daily%20Report.pdf

Kostiantynivka and Andriivka (long-range UAV)

https://www.osce.org/files/2020-07-11%20SMM%20Daily%20Report.pdf

Spartak, Pikuzy, Mineralne, Vesele and Avdiivka (mini-UAV)

https://www.osce.org/files/2020-07-13%20SMM%20Daily%20Report.pdf

Special Monitoring Mission (SMM) UAV was the target of smalls arms fire in Ukraine near the western edge of Stanytsia Luhanska (mini-UAV)

https://www.osce.org/files/2020-07-13%20SMM%20Daily%20Report.pdf

1.4. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P3)

Can a police drone recognise your face? (commentary)

https://slate.com/technology/2020/07/police-drone-facial-recognition.html

Suicide drones and the future of unmanned warfare (commentary)

https://www.thedrive.com/the-war-zone/34414/we-talk-killer-drones-and-the-future-of-unmanned-warfare-with-aerovironments-steve-gitlin

US Air Force gears up for first flight test of Golden Horde munition swarms (commentary)

https://www.defensenews.com/air/2020/07/13/air-force-gearing-up-for-first-flight-test-of-golden-horde-munition-swarms/

6th generation fighter jets to be equipped with drones (commentary)

https://eurasiantimes.com/6th-gen-fighter-jets-to-be-equipped-with-laser-weapons-as-f-22s-f-35s-could-be-phased-out/

Silence from UN Security Council leads to widespread use of drones for acts of terrorism (commentary)

http://sana.sy/en/?p=196812

Real-Time and Accurate Drone Detection in a Video with a Static Background

https://www.mdpi.com/1424-8220/20/14/3856/pdf (PDF Document)

Malicious UAV Detection Using Integrated Audio and Visual Features for Public Safety Applications

https://www.mdpi.com/1424-8220/20/14/3923/pdf (PDF Document)

Anti-Intelligence UAV Jamming Strategy via Deep Q-Networks

https://core.ac.uk/download/pdf/275662601.pdf (PDF Document)

1.5. COUNTER-DRONE SYSTEMS (P4)

Gdynia Port, Poland, selects Advanced Protection Systems' CTRL+SKY counter drone systems for port protection

https://www.linkedin.com/posts/advanced-protection-systems-sp%2E-z-o%2Eo%2E_portgdynia-antidrone-cuas-activity-6687385842849259520-CFkU

Citadel Defense networked Titan counter UAS system with AI-powered software is able to protect against 98% of COTS drones

https://www.unmannedairspace.info/counter-uas-systems-and-policies/networked-counter-drone-systems-boost-protection-provided-by-citadel/

Ruselectronics Group develops Ataka-Trophy, a mobile anti-drone system with 'friend or foe' principle

https://tass.com/economy/1178349

1.6. UTM SYSTEMS (P4)

ICAO holds RFI for submission of information for development of UTM systems

https://avia.gov.ua/wp-content/uploads/2020/06/Revised-RFI-deadline-25-Sept-2020.pdf (PDF Document)

DroneLogbook and AirMarket release a new compliance and airspace management solution for US - Canadian cross border drone operations

https://dronelife.com/2020/07/14/dronelogbook-and-airmarket/

FAA signs agreement with Swiss FOCA on UTM concept and standards for integration of drones into civilian airspace

https://www.aviationtoday.com/2020/07/10/faa-partners-swiss-authority-advance-harmonize-drone-integration-efforts/

General Electric's AiRXOS to help define architecture, standards and implementation of UAS into the national airspace

https://insideunmannedsystems.com/up-close-with-airxos/

FAA to discuss on LAANC and UTM concepts with Japan, Netherlands and Australia

https://www.unmannedairspace.info/latest-news-and-information/faa-in-talks-with-japan-the-netherlands-and-australia-in-exporting-laanc/

1.7. SOCIALS (P4)

Two civilians injured from drone strike on town in Southern Idlib, Syria

https://twitter.com/almohrarmedia2/status/1283068893171519490?s=20

Video of Saudi Arabia's F-15 shooting down Iranian drones over Yemen

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

Building a wireless war driving drone from scratch (request)

https://www.facebook.com/groups/majordomo/permalink/10160233311244522/

1.8. INFORMATIONAL (P4)

Kansas State University to offer a Master's Degree with concentration on UAS Cybersecurity

https://digitalguardian.com/blog/cybersecurity-higher-education-top-cybersecurity-colleges-and-degrees

FAA releases job role for National Security Programs and IR including UAS Security duties

http://federalgovernmentjobs.us/jobs/Director-Office-Of-National-Security-Programs-and-Incident-Response-573038500.html

Indian Oil Corporation to use RPAS for surveillance of pipelines in Mathura-Jalandhar region

https://www.hindustantimes.com/cities/pilferage-drones-to-keep-vigil-on-mathura-jalandhar-oil-pipelines/story-Njyg1pqelBsQcrZxTUYVhK.html

Two suspects armed with machete apprehended in Dudley, England, with help from police drones

https://www.stourbridgenews.co.uk/news/18578810.machete-suspects-arrested-dudley-thanks-drone-technology/

Sawyer County PD finds teenager and crashed car in a swamp with thermal imaging drone

https://www.weau.com/2020/07/14/20-year-old-injured-after-crash-thermal-imaging-found-him-in-swamp/

Volansi VTOL drone (VOLY M20) selected by US Air Force as showcase solution at AFWERX Fusion

https://volansi.com/volansi-vtol-drone-selected-by-united-states-air-force-for-afwerx-fusion-2020/

Indian Army looks into acquiring RQ-11 Raven and Spike Firefly loitering munition

https://www.hindustantimes.com/india-news/army-looks-to-acquire-us-aerial-vehicle-to-strengthen-infantry/story-vY4Cn0fZDAofyij2b0LvbN.html

US DoD awards USD $13.4Mil to AirMap, ModalAI, Skydio, Graffiti Enterprises and Obsidian Sensors to sustain development of drone capabilities

https://www.defense.gov/Newsroom/Releases/Release/Article/2270498/dod-announces-844-million-in-defense-production-act-title-iii-covid-19-actions/

RAWview and FlytBase collaborate for drone security guard and automation system

https://rawview.co.uk/blog/rawview-flytbase-press-release/

US DoD selects Northrop Grumman Forward Area Air Defense Command and Control (FAAD C2) system for future sUAS procurements

https://news.northropgrumman.com/news/releases/northrop-grumman-short-range-air-defense-system-selected-as-command-and-control-for-us-forces-to-counter-aerial-threats

1.9. DRONE TECHNOLOGY (P5)

EHang trials autonomous drone passenger flight over East China Sea

https://www.ehang.com/news/663.html

Skydio releases new X2 drone for government agencies and military usage

https://medium.com/skydio/skydio-introduces-the-new-x2-family-of-drones-and-breakthrough-autonomy-software-for-situational-499ed1ad6c11

Parrot partners with Hoverseen for development of drone-in-a-box solution for ANAFI drone

https://blog.parrot.com/2020/07/08/hoverseen-partnership/

Emesent launches first plug and play autonomous mapping payload for DJI Enterprise drones

https://www.zdnet.com/article/csrios-data61-alumni-emesent-is-flying-drones-beyond-line-of-sight/

Alpha Unmanned Systems spy UAV's achieve ISO 9001 certification

https://www.unmannedsystemstechnology.com/2020/07/alpha-unmanned-systems-achieves-iso-9001-certification/

Extending the range of delivery drones via existing transit networks (commentary)

https://earth.stanford.edu/news/could-drones-deliver-packages-more-efficiently-hopping-bus#gs.a3q5vt

Coronavirus gives urgency to Israel's national drone delivery project (commentary)

https://www.haaretz.com/israel-news/business/.premium-coronavirus-gives-urgency-to-israel-s-national-drone-delivery-project-1.8981673

General Atomics partners Asia Air Survey to validate SeaGuardian's maritime capabilities for Japan Coast Guard

https://www.ga.com/ga-asi-conducts-jcg-validation-flights-in-japan

APPENDIX A: THREAT NOTIFICATION MATRIX

A.1. OBJECTIVES

The sole focus of this service is to supply organisations with key evidence, alerts and intelligence relating to (1) Drones, (2) Counter-UAS and (3) Universal Traffic Management (UTM) systems. Together, these three items are referred to as: **DCU**. This intelligence provides a defensive net for early warning systems, fine-tuning systems based on trends and providing agencies with factual evidence in support of selecting or rejecting the need for counter-solutions. High priority will be given for the following artefacts:

- Unfolding situations or incidents relating to DCU;
- Private or public-based vulnerabilities, exploits or attack vectors affecting DCU;
- Global or national regulatory changes affecting DCU;
- Remarkable vendor or brand-specific news releases.

If an artefact is released that is considered the highest priority level (P1), Notify customers will receive an email alert linking them to the intelligence details located within their Notify portal account.

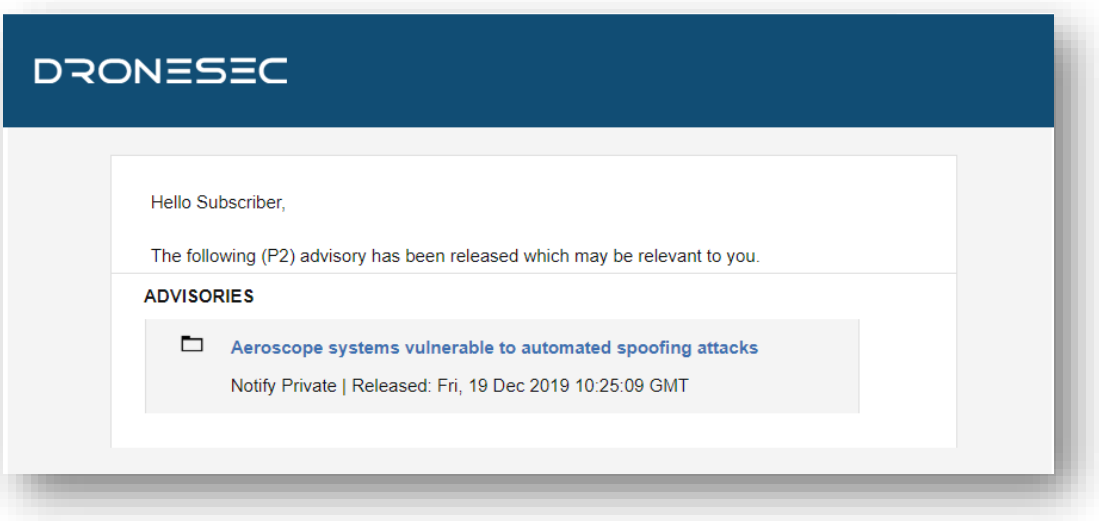


Figure 1 - A threat notification specific to a Notify customer's listed keywords.

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

Threat notifications are prioritised based on the following table:

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

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

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

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

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

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

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

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

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

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

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

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

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

APPENDIX B: SOURCES & LIMITATIONS

B.1. INTELLIGENCE SOURCES

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

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

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

B.2. LIMITATIONS

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

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

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