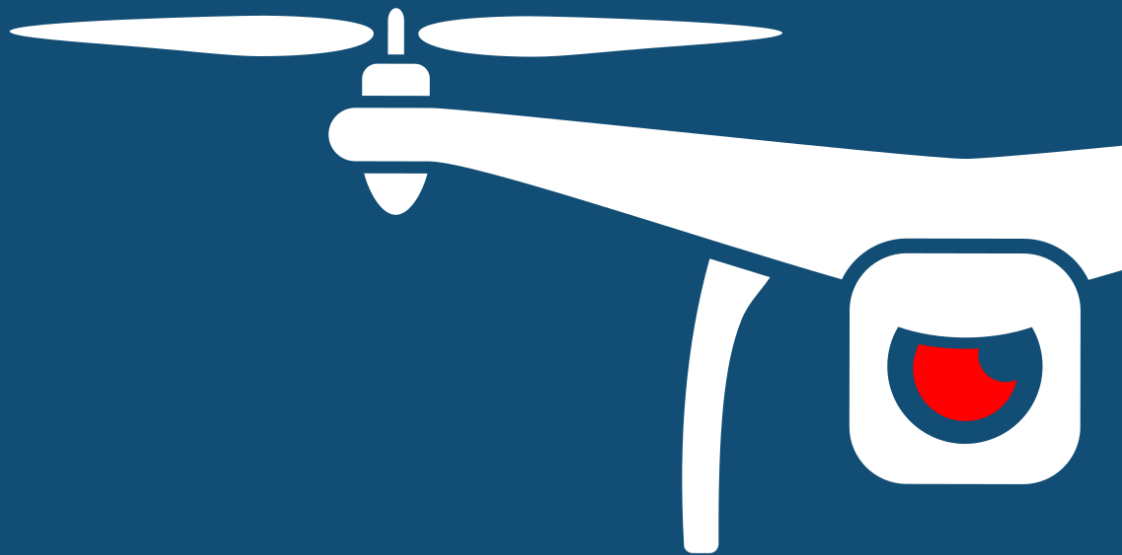




NOTIFY ISSUE #62 (PUBLIC)

WEEKLY THREAT INTELLIGENCE

17 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

We are pleased to announce the Notify **PRIVATE** subscription is now available to all users.

What is it?

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 almost 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

How much does it cost?

\$99 AUD per year. That's roughly \$1.90 per weekly issue. A single license covers an entire organisation.

Why is this being offered?

Whilst providing readers an alternative to using the real-time Notify platform, we are also increasing our analysis and reporting capability. The team have determined a fair price that will support the new quality and breadth of research involved in the incoming PRIVATE issues.

Previously, Notify PRIVATE has only been offered to Notify Platform subscribers, training students and by invitation only.

What will happen if I don't purchase a PRIVATE subscription?

You will continue to receive the PUBLIC weekly UAV Threat Intel newsletter. As of next week, it will no longer include Featured Reports or Monthly Roll-Ups.

Weekly...I want a real-time dashboard of global drone incidents?

You're after our Notify UAV Threat Intelligence Platform (<https://dronesec.com/pages/notify>) – email us to receive a demo and trial.

What do I need to do?

If you decide to join PRIVATE, sign up with the same email address you received this from.

[SUBSCRIBE TO NOTIFY PRIVATE HERE](#)

Payment/Card security?

We do not capture or store card details. We use Stripe (<https://stripe.com/>) as our payment gateway.

Thank You

To those of you who decide to join us and support the next phase of our journey, we thank you. For those that don't, we will continue to maintain the free newsletter with the same level of quality, dedication and consistency as before.

- *The DroneSec Team*



TABLE OF CONTENTS

1. Threat Intelligence -----	5
1.1. Introduction -----	5
1.2. Featured Advisories -----	6
1.3. News and Events (P3) -----	9
1.4. Socials (P3) -----	10
1.5. Whitepapers, Publications & Regulations (P3)-----	10
1.6. Counter-Drone Systems (P4) -----	10
1.7. Informational (P4) -----	11
1.8. Drone Technology (P5) -----	11
1.9. UTM Systems (P5)-----	12
APPENDIX A: Threat Notification Matrix-----	13
A.1. Objectives -----	13
APPENDIX B: Sources & Limitations -----	17
B.1. Intelligence Sources-----	17
B.2. Limitations-----	18



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.

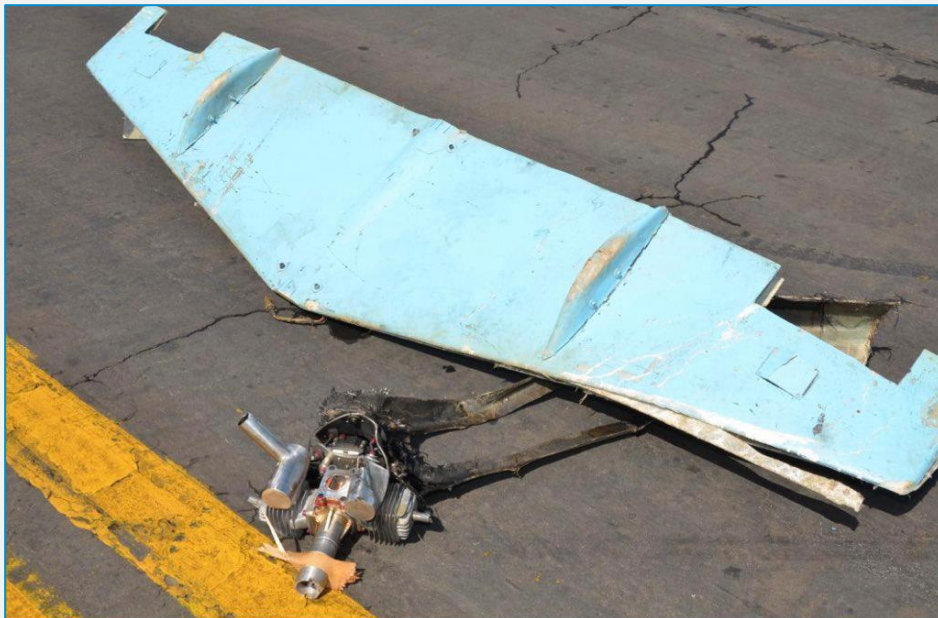


1.2. FEATURED ADVISORIES

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
Houthi drone strike hits civilian plane at Abha International Airport, Saudi Arabia	P2
<p>Summary</p> <p>A civilian Airbus A320 was hit by a suicide drone launched by the Houthi terror group. The fuselage was punctured however no casualties occurred.</p> <p>Overview</p> <p>Over the past week, Yemen's Iran-backed Houthi terror group launched multiple drone strikes against Saudi Arabia. Drones were targeting civilians and commercial installations. Abha International Airport was one of the targets that the Houthi regularly target at with their Qasf and Sammad suicide drones. In the recent attack, four drones were launched targeting Abha Airport with one of the Qasf suicide drones successfully flying straight into a civilian Airbus A320 passenger plane owned by the carrier FlyADeal.</p> <p>The drone caused a gaping hole in the rear fuselage of the commercial plane causing a fire. The fire was put out with no casualties and the Houthis claimed responsibility of the attack via their Twitter social media.</p>	
	



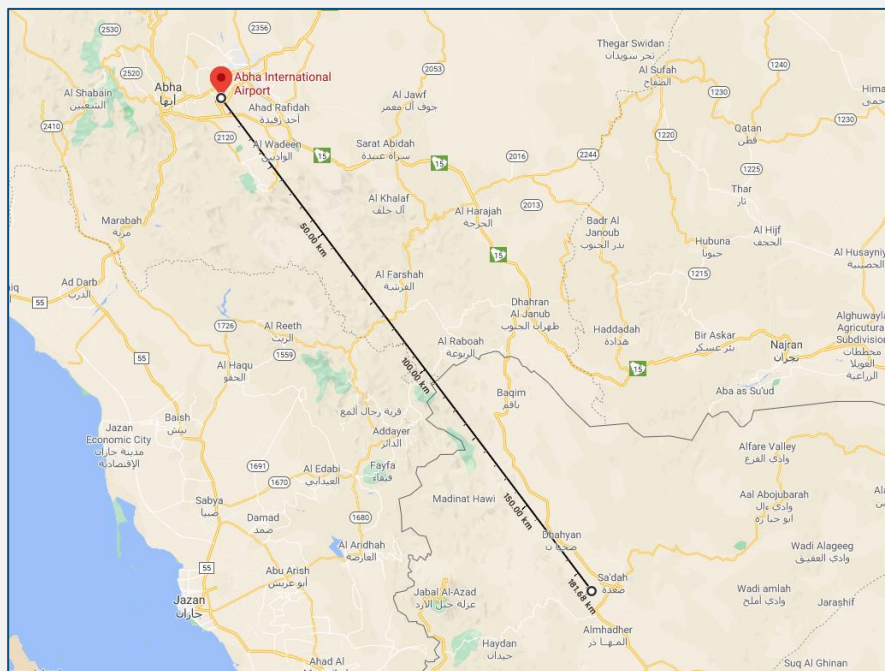


Analysis

- The Sammad and Qasef drones are said to be able to fly as far as 124miles (200km) and 1,050miles (1,700km) respectively. With these distances, it is relatively easy for the Houthis to launch their drones from cities nearing the Saudi Arabia-Yemen border such as Sada.
- Drones can be a deadly weapon even without any explosive payloads. At high speeds, they can pierce and damage objects such as windshields and metal bodies.

Drone strikes are becoming more of a common tactic for terror groups. First made popular by the Islamic State (ISIS), more terror groups are starting to see the benefits and damage drones can cause. This is a cause for concern due to the lack of counter drone infrastructure protecting cities and critical facilities. While drones used to be a military asset a decade ago, the commercialisation of quadcopters and micro drones have allowed drones to be easily purchased by threat actors and hobbyist alike. With this, anyone can have the potential to carry out misdeeds with drones. Contraband deliveries into restricted areas, drone strikes into critical infrastructure, and intrusion and surveillance on private properties are some of the nefarious use cases with drones.





Recommendation

Law enforcement agencies and governments are having difficulty in clamping down on these cases as counter drone systems are expensive and the use of these systems infringes into multiple existing policies such as Communication, Aviation and Cyber. Drones are cyber-physical systems, akin to a flying computer, and a wholistic view of all these policies are required for counter drone systems to be effective without affecting existing ones.

For now, the recommendation would be to have drone management Standard Operating Procedure (SOP) or Incident Response Plan (IRP) to mitigate against potential drone incursions. The SOP or IRP should aim to govern the process, people and methodology in responding and handling drones and the operators, collecting evidence and responding to potential drone incidents/drone operators in a pre-determined radius around the prison grounds. In addition, all incidents should be logged and categorised. This information can aid security officers in practicing and timing their response during an incursion and surface any challenges faced in communication and regulatory requirements.

References

<https://thearabweekly.com/houthi-drone-strike-hits-civilian-plane-saudi-airport>

<https://www.thedrive.com/the-war-zone/39186/yemens-houthi-rebels-strike-airliner-in-new-drone-attack-on-saudi-airport>

<https://twitter.com/SaudiEmbassyUSA/status/1359550540506673156> (images)

<https://twitter.com/SaudiEmbassyUSA/status/1359550551458013185> (images)

Want featured reports like these with detailed analysis and breakdowns? Join Notify PRIVATE!



1.3. NEWS AND EVENTS (P3)



Figure 1 - Palestinian resistance fighters shoot down Israeli quadcopter near Gaza Strip

<https://en.abna24.com/news//palestinians-shoot-down-another-israeli-drone-in-gaza-1115970.html>

Several Israelis suspected for the manufacturing, smuggling and sale of loitering suicide drones

<https://www.israelhayom.com/2021/02/11/israelis-suspected-of-illegally-building-selling-drone-missiles-to-asian-country/>

Manned pilot spots two drones flying at 700ft near Boundary Bay Airport, Canada

<https://avrodex.com/view/2021P0141>

Man arrested for smuggling four DJI Phantom 4 drones into India from UAE

<https://www.newindianexpress.com/cities/bengaluru/2021/feb/11/dubai-passenger-flies-in-with-four-drones-caught-2262455.html>

Arab Coalition destroys three Houthi suicide drone targeting civilians

<https://saudigazette.com.sa/article/603501/SAUDI-ARABIA/Coalition-forces-intercept-destroy-2-Houthi-fired-drones>

Interception of Houthi drone leaves shrapnel near Saudi Arabia's Abha Airport

<https://www.arabnews.com/node/1810206/saudi-arabia>

Drone strikes in Somalia kill several members of Al-Shabaab terror group

<https://intelligencebriefs.com/drone-strikes-hit-two-al-shabaab-stronghold-towns-in-sakow-and-salagle-middle-jubba/>

Drone strike destroys militia's weapon and ammunition shipment into Syria

<https://www.timesofisrael.com/drone-strike-reported-on-pro-iran-militia-arms-shipment-on-iraq-syria-border/>



1.4. SOCIALS (P3)

The PKK release footage using drones to drop home-made bombs on Turkish troops in Gare

<https://twitter.com/Conflicts/status/1361628657639436290>

Belarus unveils two swarm-capable quadcopter drones armed with RPG-26

<https://www.linkedin.com/posts/activity-6763088201298124800-nqxn/>

The dangers of drones (documentary)

<https://www.tvgids.nl/tv/de-gevaren-van-drones/103779481>

1.5. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P3)

Airservices Australia proposes to lower Class E airspace to 1,500ft for drone operations

<https://www.unmannedairspace.info/latest-news-and-information/australian-uas-association-seeks-input-on-proposal-to-lower-class-e-airspace-on-the-east-coast/>

EASA launches project assessing the vulnerability of manned aircraft from drone strikes

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

The drone defense dilemma: How unmanned aircraft are redrawing battle lines (commentary)

<https://www.defensenews.com/global/europe/2021/02/15/the-drone-defense-dilemma-how-unmanned-aircraft-are-redrawing-battle-lines/>

Talking Horses: Drone wars over UK racetracks (commentary)

<https://www.theguardian.com/sport/2021/feb/12/drone-wars-over-uk-racetracks-after-courses-say-live-streams-are-illegal-horse-racing-tips-talking-horses>

Strategic approach – Reducing risk of rogue drones (commentary)

<https://crisis-response.com/Publisher/Article.aspx?ID=602507>

Remote ID For Manned Aviators (commentary)

<https://www.suasnews.com/2021/02/remote-id-for-manned-aviators/>

Drone swarms versus stealth covers are the future of warfare (commentary)

<https://www.livemint.com/news/business-of-life/drone-swarms-versus-stealth-covers-are-the-future-of-warfare-11613314693054.html>

1.6. COUNTER-DRONE SYSTEMS (P4)

Phantom Technologies unveils RF-jamming counter drone system, Phantom Dome 180

<https://www.israeldefense.co.il/en/node/48320>

French Air Force receives Nerod F5 jammer rifles and training for anti-drone unit

<https://www.defense.gouv.fr/air/actus-air/de-nouveaux-materiels-de-derniere-generation-pour-l-escadron-de-protection-d-istres>



Russian Almaz-Antey tests interceptor drone, Volk-18, with three net launchers armament

<https://www.unmannedairspace.info/counter-uas-systems-and-policies/almaz-antey-tests-interceptor-drone-designed-to-take-out-enemy-drones/>

US Air Force tests Raytheon's laser weapon system designated to counter drone threats

<https://www.wpafb.af.mil/News/Article-Display/Article/2503929/directed-energy-ctf-oversees-testing-of-anti-drone-weapon/>

Russian defence giant Almaz-Antey completes testing of new drone hunting interceptor UAV

<https://www.uasvision.com/2021/02/15/russia-completes-testing-of-new-drone-hunting-uav/>

1.7. INFORMATIONAL (P4)

Drones employed to search for two escapees from a rehabilitation center, Kearney

https://theindependent.com/news/state-and-regional/law-enforcement-use-drone-to-search-for-two-yrtc-escapees-tuesday/article_4d5bb28c-289a-5bda-864a-c8e48732fb5c.html

Drone helps officials rescue hiker stuck on Table Mountain

<https://www.iol.co.za/capeargus/news/drone-helps-officials-rescue-hiker-stuck-on-table-mountain-eb002cc2-4d30-4aea-911f-c8cb897508d7>

Lauderhill Firefighters utilise thermal drone to identify hotspots for extinguishing

<https://dronestoday.org/blog/thermal-drone-helps-firefighters-battle-blaze-in-home/>

Bomb squad used drone to identify suspicious package found on road in Santa Clara County

<https://sanfrancisco.cbslocal.com/2021/02/13/drone-deployed-to-examine-suspicious-device-on-stevens-creek-trail/>

Morocco to order drones from Israel's IAI and BlueBird Aero Systems

<https://www.moroccoworldnews.com/2021/02/335118/morocco-orders-drones-from-israels-bluebird-aero-system/>

Novadem to deliver another 50 NX70 drones to French Army, totalling 200 microdrones

https://www.armyrecognition.com/defense_news_february_2021_global_security_army_industry/novadem_to_deliver_about_50_more_nx70_microdrones_to_french_army_in_2021.html

1.8. DRONE TECHNOLOGY (P5)

GPS-denied drone delivery successfully tested in Israel

<https://www.jpost.com/jpost-tech/israel-carries-out-first-ever-worldwide-drone-test-without-gps-succeeds-658886>

India and Israel to collaborate and produce SkyStriker loitering munition

<https://bangaloremirror.indiatimes.com/bangalore/others/bengaluru-israel-firms-to-produce-suicide-drones/articleshow/80867148.cms>



Armenia to test indigenous suicide drone after lessons from conflict with Azerbaijan

<https://www.thedefensepost.com/2021/02/12/armenia-tests-kamikaze-drone/>

Leonardo trials electric powered drone for BVLOS and heavy weight delivery capabilities

<https://www.leonardocompany.com/en/press-release-detail/-/detail/12-02-2021-leonardo-carries-out-italy-s-first-demonstration-of-a-drone-with-electrically-powered-propulsion-transporting-heavy-goods>

FlytBase and Heisha Tech collaborate to offer low-cost drone-in-a-box solution

<https://www.geospatialworld.net/news/flytbase-heisha-collaborate-to-offer-a-low-cost-automated-drone-in-a-box-solution/>

1.9. UTM SYSTEMS (P5)

The UTM industry is facing a financial crisis – business models no longer work (commentary)

<https://www.unmannedairspace.info/commentary/the-utm-industry-is-facing-a-financial-crisis-business-models-no-longer-work/>

Altitude Angel and Inmarsat wins award with their Pop-Up UTM concept

<https://www.altitudeangel.com/news/posts/2021/february/altitude-angel-inmarsat-ground-breaking-pop-up-utm-wins-2020-atm-award/>

NUAIR issues RFI for New York drone corridor for UTM development

<https://dronelife.com/2021/02/15/nuair-issues-utm-rfi-long-term-development-of-the-new-york-drone-corridor/>



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.

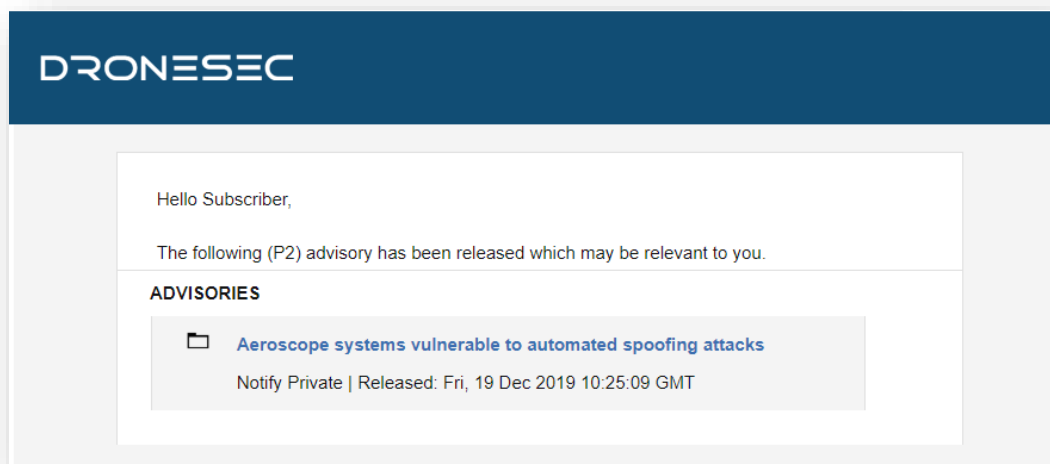


Figure 2 - A threat notification specific to a Notify customer's listed keywords.

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: <ul style="list-style-type: none">• Be known as UAS¹, UAV², RPAS³...• Weigh 50g all the way to 250kgs• Are automated or manually piloted• Have associated devices, software or infrastructure
CUAS	Counter-UAS systems that might: <ul style="list-style-type: none">• Be known as Counter-Drone or C-UAV

¹ UAS: Unmanned Aerial System

² UAV: Unmanned Aerial Vehicle

³ RPAS: Remotely Piloted Aerial System



	<ul style="list-style-type: none"> • Detect and/or respond to drones • Be standalone, hand-held, static or integrated with a UTM⁴ or PSIM⁵ system • Have associated systems, software, infrastructure and communication protocols
UTM	Universal Traffic Management system that might: <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> - 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 dronsec.xyz, dronsec.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@dronsec.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.

