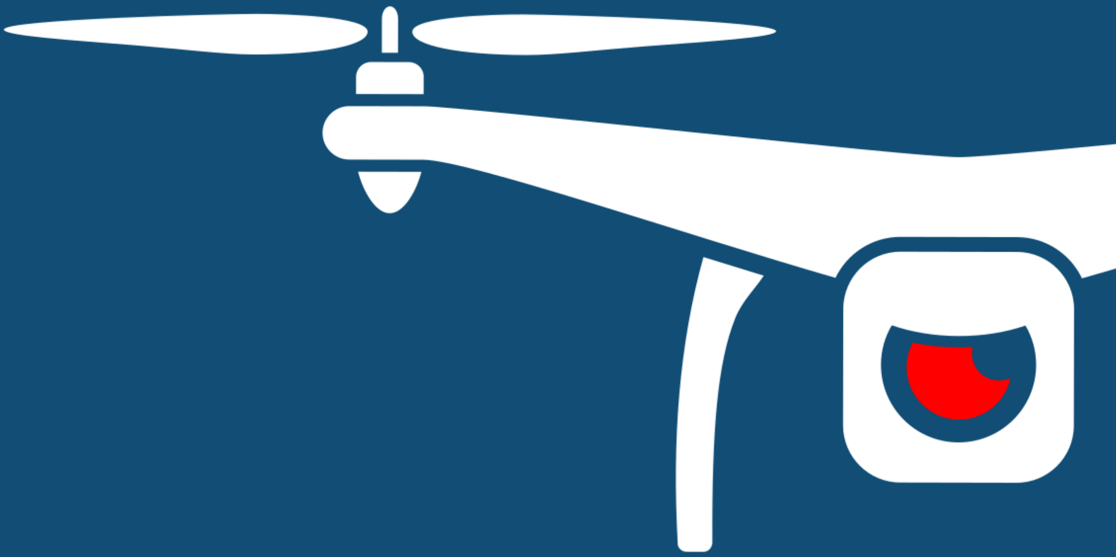
NOTIFY ISSUE #15

WEEKLY THREAT INTELLIGENCE

25 March 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

Lots of COVID-19 related content this week, specifically regarding the innovative use of drones with disinfectant. A good use case for our filters for sure, trying to gauge how much of this information is meaningful (e.g. the many makes and models used by law enforcement agencies) vs the fact that we've probably seen all these reports a hundred times over by now!

Obviously however, it's great to see thermal, voice and vision drones getting so much use by Emergency Services during the pandemic and we're sure many more use cases will emerge. The team enjoyed sharing some light-hearted videos of various drone uses not seen before, such as dropping car keys, delivering flowers and walking dogs via drone; obviously whilst shaking heads at the legality of it all!

Things are heating up on the Indo-Pakistani border, with almost daily events of small, rogue COTS drones being spotted or apprehended smuggling weapons and contraband. The Indian military have been looking into Counter-UAS systems for some time, yet are struggling to capture a perimeter environment as long and wide as that being monitored against threats to Punjab.

- *Mike Monnik, DroneSec CTO*

TABLE OF CONTENTS

1. Threat intelligence ---------- 5
1.1. Introduction ---------- 5
1.2. Featured Advisories (P2) ---------- 6
1.3. News and Events (P3) ---------- 7
1.4. Whitepapers, Publications & Regulations (P3)---------- 7
1.5. Counter-Drone Systems (P4) ---------- 8
1.6. UTM Systems (P4) ---------- 8
1.7. Drone Technology (P5) ---------- 8
1.8. Informational (P5) ---------- 9
APPENDIX A: Threat Notification Matrix---------- 10
A.1. Objectives ---------- 10
APPENDIX B: Sources & Limitations ---------- 14
B.1. Intelligence sources ---------- 14
B.2. Limitations---------- 15

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.

Kicking it all off, we're delivering our first few rounds in PDF format. In the next few weeks, we'll continue to roll out platform access to ensure we can sustainably support our current client needs with relevant, actionable information within the context of DCU.

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 (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.

Security	Tags	Priority
Nine terrorists charged for dropping arms and ammunitions in Punjab across Pakistan border	Drones, Border Infringement, Contraband	P2

Summary

Nine members of the Khalistan Zindabad Force (KZF) terror group were charged for smuggling ammunitions, explosives, counterfeit money and firearms to Punjab via drones from Pakistan.

Overview

The KZF terror group were plotting a terror attack to create disharmony and communal tension in Punjab and had recruited nine members ranging from the age of 20 to 70. A total of eight drone flights were carried out since August 2019 which saw contraband items transported via drones across the Pakistan-Punjab border. Items include explosives, ammunition and firearms, communication devices and counterfeit notes. The terror attack was planned in Amritsar Central Jail in 2018 when one of the members, Akashdeep, was recruited by KZF loyalists while in custody with them for other crimes.

Analysis

Drones and their controllers are linked via wireless communication and with the low price point and availability of COTS drones nowadays, conducting illegal acts can happen at an easier rate without risk undertaken by the offender on being apprehended. Furthermore, the skill barrier to be able to fly a drone is not complex, and incidents often see offenders becoming lax with their approach and utilising the same take-off/landing points as before. Monitoring the drones and recognising patterns and trends may divulge the modus operandi of rogue groups and result in the arrest the organisation rather than individual actor or operator.

Recommendation

All perimeter defences should have a Drone Security Management Plan in place to deal with small unmanned systems, whether counter-drone systems are in place within the environment. A standard operating procedure (SOP) should govern the process, people and methodology in handling drones, collecting evidence and responding to potential rogue operators and their accomplices around the perimeter grounds.

Any incident should be logged, categorised and reported to local law enforcement. Event tracking and analysis should take place by determining if the drone and its flight path was similar to previous cases. This information can be analysed for common trends and patterns to aid enforcement agencies in apprehending operators when faced with illegal contraband delivery.

Finally, environments that include counter-drone systems in their perimeter security should combine these systems with data analytics, tracking and post-incident analysis capabilities in order to enhance proactive security efforts.

References

- https://www.firstpost.com/india/nia-files-chargesheet-against-9-khalistani-terrorists-in-punjab-drone-arms-drop-case-8165521.html

1.3. NEWS AND EVENTS (P3)

Syria shoots down rogue drone in vicinity of Russia's Hmeimim air base

https://www.albawaba.com/news/drone-shot-down-near-russias-airbase-syrias-hmeimim-1346536

China deploys 12 underwater drones in Indian Ocean for naval intelligence

https://www.forbes.com/sites/hisutton/2020/03/22/china-deployed-underwater-drones-in-indian-ocean/#3f14b8e26693

Drone spotted and fired upon at Indo-Pakistan border in Ramgarh, India

https://www.indiatoday.in/india/story/indo-pak-border-drone-1636762-2020-01-14

Drones to integrate with Belarus SWAT for reconnaissance and ambushing tactics

https://belsat.eu/en/news/belarusian-swat-now-armed-with-drones/

India suffers multiple Pakistani-based international border crossings by small drones

https://sputniknews.com/india/202003191078620766-india-accuses-pakistan-of-air-space-violation-as-drone-crosses-international-border/

https://sputniknews.com/india/202002131078303960-threat-of-attack-from-swarm-of-drones-looms-large-in-indias-border-state-/

Kansas, USA police deploys drone to track and arrest burglar

https://salinapost.com/posts/5e712277afae0f4d5f5d52b0

1.4. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P3)

Analysing Drone's RCS at different frequencies to improve drone detection radars (IEEE)

https://ieee-dataport.org/open-access/drone-rcs-measurements-26-40-ghz

https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9032332 (PDF Document)

Senator Markey queries FAA on local state authority testing of counter-drone technology

https://www.markey.senate.gov/news/press-releases/senator-markey-queries-faa-about-local-authority-to-test-counter-drone-technology

Counter-Unmanned Aircraft Systems Technology Guide – Homeland Security

https://www.dhs.gov/sites/default/files/publications/c-uas-tech-guide_final_28feb2020.pdf

The Drone Pilots Legal Handbook

https://www.linkedin.com/posts/tom-pils-809a6952_the-drone-pilots-legal-handbook-activity-6647278935585488896-RK56

1.5. COUNTER-DRONE SYSTEMS (P4)

Canadian Navy tests and evaluates onboard counter-drone systems against small rotor drones

https://www.unmannedairspace.info/counter-uas-systems-tenders/canadian-navy-works-tests-counter-drone-measures-using-technology-supplied-by-qinetiq/

Nigeria to consider anti-drone systems to counter drone terrorism

https://guardian.ng/news/senate-recommends-anti-drone-systems-to-counter-terrorism/

1.6. UTM SYSTEMS (P4)

Chinese drone maker EHang collaborates with Spain for unmanned air mobility pilot programme

https://bingepost.com/chinese-aerial-drone-manufacturer-makes-first-foray-into-spain/65791/

1.7. DRONE TECHNOLOGY (P5)

Obstacle avoidance tech from University of Zurich reduces drone reaction time to 3.5ms

https://newatlas.com/drones/drone-dodgeball-obstacle-detection-system/

China deploys several unmanned underwater drones into the Indian ocean

https://www.forbes.com/sites/hisutton/2020/03/22/china-deployed-underwater-drones-in-indian-ocean/#3c8ac7b16693

Commtact successfully demonstrated a wireless datalink for BVLOS drone flights up to 16km

https://www.unmannedsystemstechnology.com/2020/03/wireless-datalink-integrated-into-bvlos-uav/

3G network and intermittent cellular communications can still support complex drone operations

https://www.unmannedairspace.info/news-first/intermittent-cellular-communications-can-still-support-complex-drone-operations-gutma-connected-skies-webinar/

Jammu and Kashmir PD deploy Mavic 2 and Phantom 4 drones with thermal camera to restrict movement during 10-day lockdown

https://www.thekashmirmonitor.net/thermal-drones-to-be-used-to-check-movement-igp-kashmir/

Karimnagar, India, deploys Marut drones to spray disinfectant and reduce personnel contact

https://telanganatoday.com/karimnagar-to-have-drone-solution-for-covid-19

Drones used in Greece to monitor movement control during virus lockdown

https://greekcitytimes.com/2020/03/23/drones-will-monitor-citizens-to-ensure-compliance-to-lockdown-laws/

Italian Armed Forces activated with drones to monitor citizen during restricted movement order

https://www.breitbart.com/europe/2020/03/22/italian-police-deploy-drones-to-track-and-arrest-lockdown-violators/

Kildare North, Ireland, deploys drones to disperse crowd and control movement

https://www.leinsterleader.ie/news/news/528542/kildare-td-proposes-drones-to-police-social-distancing.html

Chula Vista PD, California, fits Matrice 210 and Mavic 2 Enterprise with thermal vision to enforce restricted movement order

https://www.washingtonexaminer.com/news/california-police-to-use-chinese-made-patrol-drones-with-night-vision-cameras-during-coronavirus-lockdown

Dubai and Sharjah Police uses Mavic 2 to remind citizens to stay home during virus pandemic

https://www.thenational.ae/uae/government/coronavirus-police-use-loudspeaker-drones-to-say-stay-home-in-multiple-languages-1.996171

1.8. INFORMATIONAL (P5)

Queensland Department of Agriculture and Fisheries uses Phantom 4 for pasture surveillance

https://www.farmonline.com.au/story/6687564/measuring-pasture-intake-with-drones/

Throttle Aerospace Systems and Dunzo gets green light for drone delivery experiment, India

https://timesofindia.indiatimes.com/india/2-drones-built-in-bengaluru-get-dgca-nod-for-delivery-experiment/articleshow/74699187.cms

New Zealand firm Dotterel creates drone noise reduction technology

https://www.suasnews.com/2020/03/high-flying-japanese-fund-invests-in-dotterel-uav-acoustics/

Singer deliver music albums via drone delivery

https://people.com/country/kelsea-ballerini-delivers-album-pizza-drone/

Geely offers delivery of new car keys via drones to reduce contact between personnel

https://www.carscoops.com/2020/03/geely-now-uses-drones-to-deliver-new-car-keys-to-customers/

Video displays dog being walked by drone amidst coronavirus lockdown

https://www.nydailynews.com/coronavirus/ny-coronavirus-drone-walks-dog-cyprus-lockdown-20200319-dvpxy46a7ncxza2kxijlu6ym6i-story.html

Celine Dion travels with drone swarm of 104 on tour

https://www.inc.com/heather-r-morgan/meet-104-drones-touring-with-celine-dion.html

Drone Search and Rescue (SAR) officers locate and rescue injured hiker

https://www.stgeorgeutah.com/news/archive/2020/03/18/cgb-multiple-crews-and-a-drone-combine-forces-to-rescue-2-hikers-hours-apart-in-red-cliffs-reserve/#.XnRQj25uJEx

Iron County Sheriff looks into acquiring drones for investigation and accident scenes

https://dailyjournalonline.com/news/local/crime-and-courts/iron-county-sheriff-hopes-to-get-drone/article_e13f2c67-b63b-5d66-8ce0-c516b6de4d5e.html

Drones used to locate injured paraglider in Marlborough, New Zealand

https://www.stuff.co.nz/national/120498401/drone-assists-in-locating-paraglider-in-serious-condition-after-crash-in-marlborough

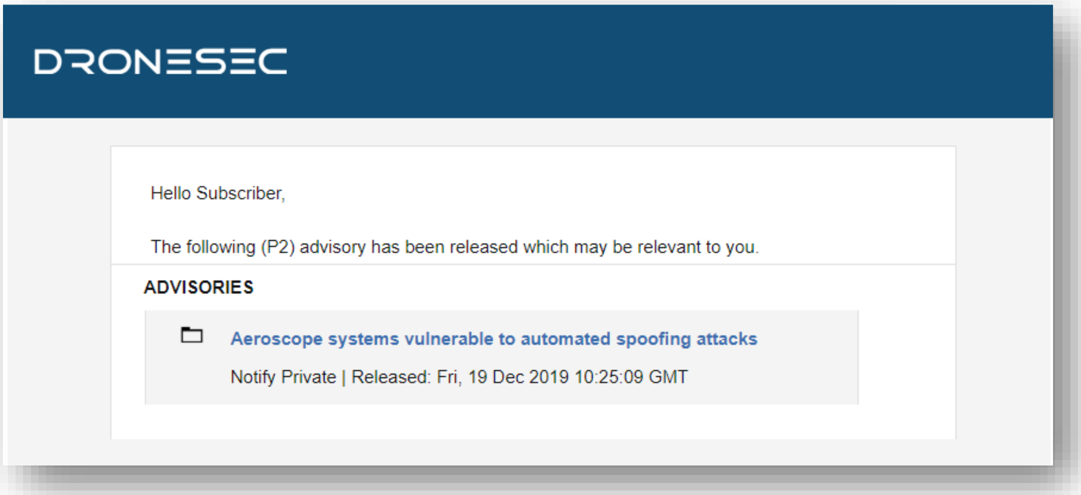
APPENDIX A: THREAT NOTIFICATION MATRIX

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.



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 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.