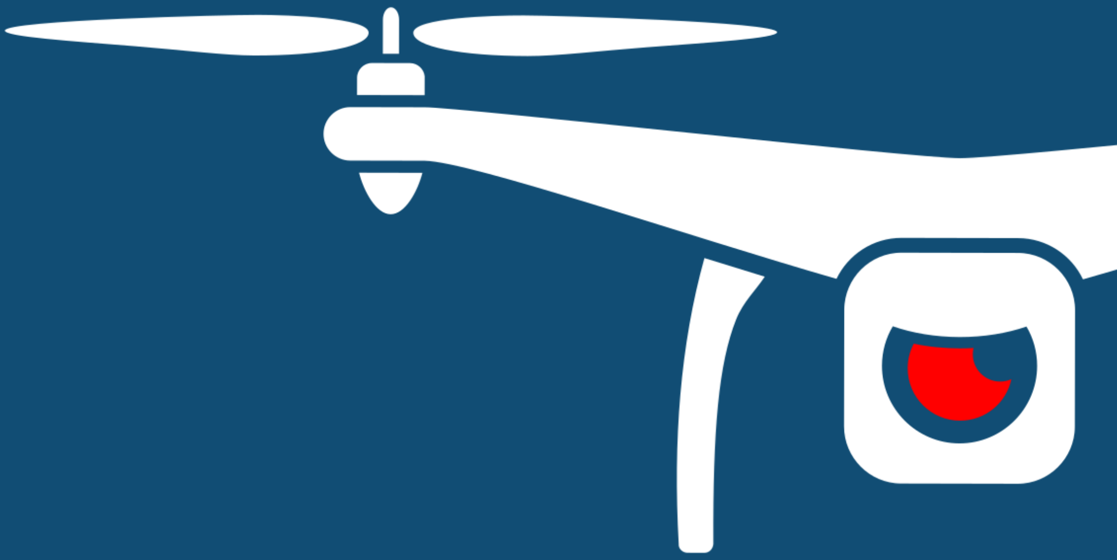
DRONE SEC
A Privasec COMPANY

NOTIFY ISSUE #19

WEEKLY THREAT INTELLIGENCE

22 April 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 added a number of new sources and priority notifications to our system – existing customers should notice this immediately and feedback is welcomed. For any of our free subscribers, you can find out more information about our paid platform by contacting us at info@dronesec.com.

You may notice our reporting style has changed slightly also – we are ensuring that drone make, model and types are adequately sourced (whether they appear in the source or not) and acknowledged. Previously, we have been silently cataloguing these in our database; extracting key information such as the types of drones in use by different organisations to provide insights. By making these available to the public, their security teams can make quicker and more effective decisions about their defensive posture.

Going through the highlights of the week, we see an event where a missing Law Enforcement drone is being searched for by… more drones. The drones are being used to detect drone-like shapes in order to locate the missing drone; certainly not the same as a missing police cruiser, but a contingency measure all Law Enforcement should expect and plan for.

We've also seen an uptick in social media sharing guides on attaching items and payloads to drones, modifying vision of non-FPV drones and more amongst COVID-19. While the meaning is innocent, we will be monitoring these closely to assess if it brings more opportunistic malicious use cases with the rise of accessible information. That being said – we're not for censoring this type of information, however it is meaningful to analyse.

A great podcast has popped up on our radar this week with a plethora of detailed information regarding UAS, their Ground Control Stations and Counter-UAS measures in Idlib, Syria. It is only 7-minutes long and well worth the listen. Otherwise, the DoT review of inadequate security control measures within the FAA has been released and acknowledged – we will be keeping a close eye on the outcomes in the near future.

As always, our slack workspace is open for discussion of all things drone, counter-drones and UTM security.

- *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.

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)

All Featured Advisories pushed to DroneSec customers this week were private.

1.3. NEWS AND EVENTS (P3)

Department of Transportation flags FAA for having lax security and privacy controls on drone user’s personal identifiable information

https://justthenews.com/government/security/faa-doesnt-have-adequate-security-over-drone-databases-personal-info-flight

https://www.oig.dot.gov/sites/default/files/FAA%20DroneZone%20Security%20Controls%20Final%20Report.pdf

Electronic Warfare in UAV/Drones and their control stations in Idlib, Syria (Commentary)

https://armadainternational.com/2020/04/electronic-warfare-podcast-2-electrons-in-idlib-741/

Russia’s BirdEye 400 shot down by Ukraine for flying too close to territorial border (UPDATE)

https://defence-blog.com/news/ukrainian-forces-shoot-down-russian-drone-in-donetsk-region.html

https://twitter.com/dmitrosel007/status/1246848861592850432

Israel drone strike on terror group Hezbollah in Syria

https://www.thedefensepost.com/2020/04/15/israel-hezbollah-drone-strike-syria-lebanon/

Artsakh Defense Army destroys intruding Azerbaijani’s Orbiter UAV

http://asbarez.com/193726/artsakh-forces-down-azerbaijani-drone-2/

Libyan National Army downs 2 Turkish drones reported targeting medical vehicles

https://aawsat.com/english/home/article/2240086/lna-downs-two-turkish-drones-bani-walid

43 USA police agencies from 22 states accept DJI donated drones to help combat COVID-19. Despite security concerns, Law Enforcement state no pictures or video recordings used.

https://www.bizpacreview.com/2020/04/17/drones-used-to-enforce-social-distancing-in-us-reportedly-donated-by-chinese-tech-company-909870

Multiple drones deployed to locate missing COVID-monitoring drone in Noida, India

https://www.newindianexpress.com/nation/2020/apr/16/drone-monitoring-corona-hotspot-in-noida-goes-missing-2130969.html

Brick Township Police, USA, locate and arrest harassment suspect with drone

https://www.app.com/story/news/2020/04/21/drone-leads-brick-police-bias-suspect/2999833001/

Indian Army tests autonomous, long-range Indian-made drones for 25km BVLOS delivery

https://www.tribuneindia.com/news/nation/army-tests-delivery-via-drones-in-punjab-73591

1.4. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P3)

FAA updates regulation on the use of drone for transportation during COVID-19 response efforts

https://www.faa.gov/coronavirus/regulatory_updates/#dure

UK CAA relaxes rules on drone operations for enforcement agencies during COVID-19 lockdown

https://www.southwalesguardian.co.uk/news/national/18381797.drones-rules-relaxed-police-enforcing-covid-19-lockdown/

UK CAA retracts relaxed drone rules, limits height from 600ft to 500ft for enforcement agencies

https://www.theregister.co.uk/2020/04/20/police_drone_fliers_wings_clipped/

Drones banned over NHS Louisa Jordan hospital, Scotland as airspace restriction placed

https://www.glasgowtimes.co.uk/news/18384554.drones-banned-nhs-louisa-jordan-police-impose-new-airspace-ban/

UK Drone Delivery Group releases whitepaper for public consultation on drone testing grounds

https://drive.google.com/file/d/1yNzX5ZFaARHlPplh9f8mup-lyLg5GGY4/view (online document file)

https://www.smarttransport.org.uk/news/latest-news/public-consultation-launched-on-drone-delivery-in-the-uk

Analysis of the GPS spoofing vulnerability in the drone 3D Robotics Solo

https://ieeexplore.ieee.org/document/8691741 (PDF Available to Notify Customers)

1.5. COUNTER DRONE SYSTEMS (P4)

Citadel Defense expands Titan AI to detect small unmanned drones

https://www.airforce-technology.com/news/citadel-defense-expands-ai-software-to-counter-drones/

DroneShield releases latest new body worn drone detection system, RfPatrol MKII

https://www.shephardmedia.com/news/digital-battlespace/droneshield-unveils-latest-body-worn-drone-detecti/

1.6. UTM SYSTEMS (P4)

Kongsberg Geospatial secures US$1.4mil contract to develop UTM for BVLOS drone operations

https://www.geospatialworld.net/news/kongsberg-geospatial-selected-for-ohio-utm-drone-project-team/

Skyports joins UK CAA for BVLOS flight trials

https://www.adsadvance.co.uk/skyports-joins-caa-regulatory-sandbox-to-trial-bvlos-flights.html

1.7. INFORMATIONAL (P5)

Parrot to manufacture short range reconnaissance drone for US Army

https://www.defenceonline.co.uk/2020/04/17/parrot-short-range-reconnaissance-drone-us-dod/

USA based Terraview qualifying to sell to U.S. government organisations in bid against DJI

https://dronelife.com/2020/04/20/a-u-s-based-dji-alternative-terraviews-rangepro/

ASYLON Inc awarded contract from USAF for persistent ISR, inspection and perimeter security

https://www.suasnews.com/2020/04/asylon-awarded-contract-for-pushing-the-limits-of-autonomous-systems-for-defense/

Norway police locate missing person through drone thermal vision

https://www.uasnorway.no/savnet-funnet-av-dronepilot-na-redder-droner-liv-ogsa-i-norge/

1.8. DRONE TECHNOLOGY (P5)

ETH Zurich design a multirotor drone with controllable motion in six degrees of freedom

https://hackaday.com/2020/04/14/the-drone-that-flies-in-any-orientation/

Drone used radio waves to remotely recharge sensors during mid-flight

https://spectrum.ieee.org/tech-talk/sensors/remote-sensing/uavs-prove-usefuldelivering-remote-power-charging-services

DroneUp and UPS uses DJI Inspire 2 to test drone deliveries of medical supplies

https://www.foxnews.com/tech/ups-droneup-test-drone-delivery-of-medical-supplies

30 private drones leased to Ahmedabad Police for enforcing of COVID-19 lockdown

https://timesofindia.indiatimes.com/city/ahmedabad/cops-use-30-private-drones-for-surveillance-deliveries/articleshow/75169453.cms

Tirana Police, Albania, use drones to enforce lockdown rules

https://www.reuters.com/article/us-health-coronavirus-albania-lockdown/drones-time-slots-give-albanias-virus-lockdown-a-hi-tech-edge-idUSKCN21Y1WC

5,000 Greek police and drones used to enforce Easter lockdown

https://www.thenationalherald.com/298999/army-of-greek-police-drones-stop-covid-19-easter-exodus/

Patna, India, uses 10 drones for movement monitoring

https://timesofindia.indiatimes.com/city/patna/district-administration-uses-ten-drones-for-surveillance/articleshow/75238350.cms

Rwanda, Africa, deploys 2 DJI Matrice 600 to monitor citizens breaching COVID-19 laws

https://www.channelnewsasia.com/news/business/rwanda-uses-drones-to-help-catch-lockdown-transgressors-12653478

Battle Creek PD receives Mavic 2 Enterprise as COVID-19 donation from DJI

https://www.battlecreekenquirer.com/story/news/2020/04/17/drones-donated-battle-creek-police-virus-fight/5151842002/

Fort Worth PD deploys Mavic 2 drone to remind homeless to keep social distancing

https://www.nbcdfw.com/news/coronavirus/fort-worth-police-deploy-drones-to-remind-homeless-about-social-distancing/2354753/

Matrice 200 drone performs deliveries in Chile, South America, to help combat COVID-19

https://www.reuters.com/video/watch/idPHjp?now=true

Rimini Local Police deploys Mavic Mini and Mavic 2 drones to enforce lockdown measures

https://www.dailymail.co.uk/news/article-8240381/Italian-police-swarm-man-sunbathing-deserted-beach-fine-breaking-lockdown-rules.html

Malavalli PD deploys Phantom 4 drones and CCTV to help arrest citizens who flout lockdown

https://www.thehindu.com/news/national/karnataka/drones-cctv-cameras-help-police-to-curb-public-movement/article31397181.ece

Westport PD, US, deploys Matrice 200, Phantom 4 and Mavic 2 to fight COVID-19

https://www.nbcconnecticut.com/news/local/westport-police-to-test-pandemic-drone-that-can-sense-fevers-coughing/2258746/

Kent County Sheriff's Department receives 4 Mavic 2 Enterprise from DJI to fight COVID-19

https://www.woodtv.com/health/coronavirus/w-mi-police-agencies-use-drones-in-covid-19-response/

300 Phantom 4 drones lights up sky in Zhuhai, China

https://www.sbs.com.au/news/300-drones-light-up-night-in-south-china-s-zhuhai-to-show-gratitude-to-medics

1.9. SOCIALS (P5)

Two men arrested for delivering tobacco-related product via DJI Mavic 2 drone, India

https://twitter.com/_anubhavk/status/1249241110485991424

Indian man demonstrates how a DJI Mavic Pro can be configured to carry items and payloads

https://youtu.be/BP9RxFx6U7w

Youtuber demonstrates how to modify Mavic Mini to support FPV goggles

https://www.youtube.com/watch?v=AHwlX9IpVRY

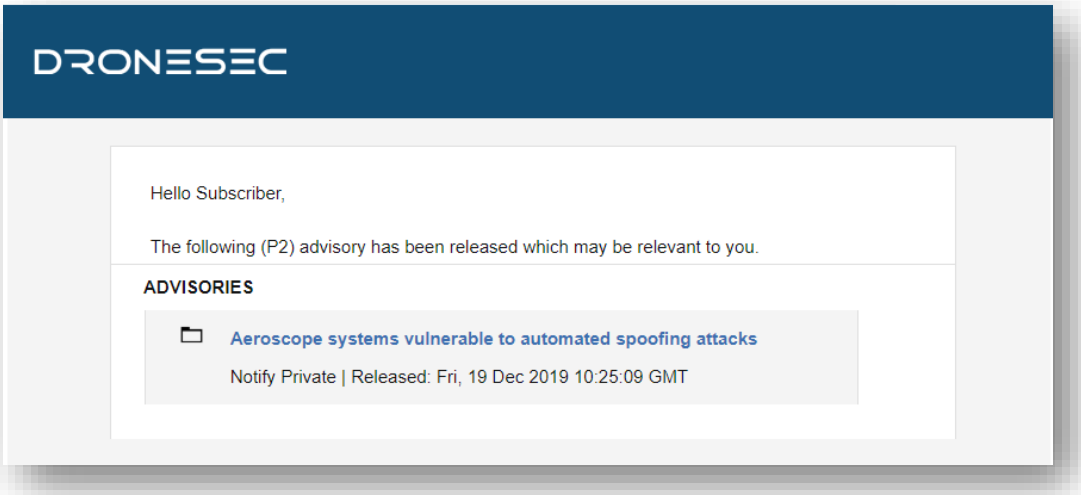
APPENDIX A: THREAT NOTIFICATION MATRIX

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.