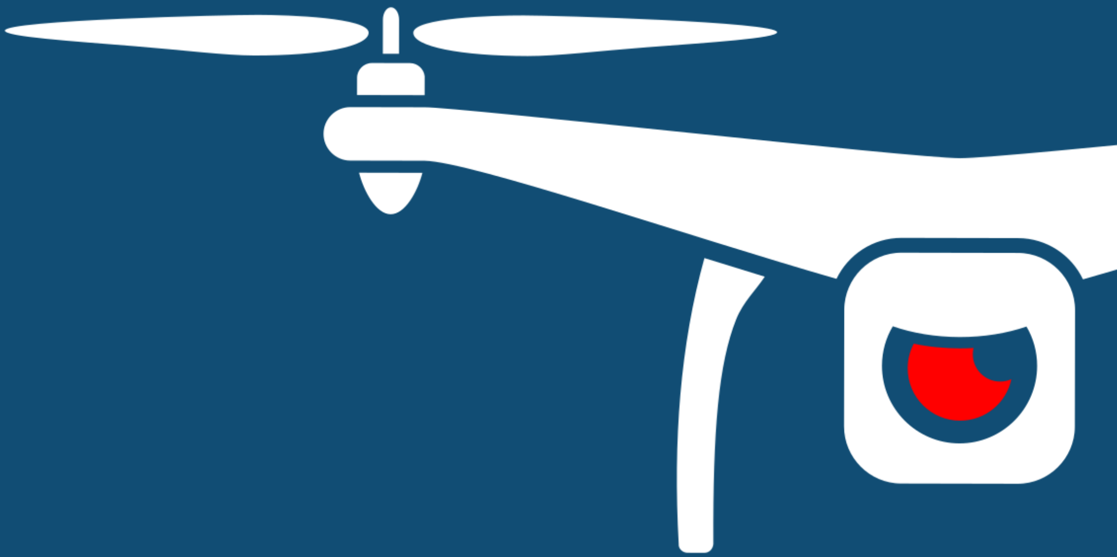
DRONE SEC
A Privasec COMPANY

NOTIFY ISSUE #16

WEEKLY THREAT INTELLIGENCE

1 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

Happy April 1st!

Another month means we undertake a roll-up and analysis of the month gone by. One of the key insights we've been able to observe is that there has been an uptick in offenders being *apprehended* by authorities compared to the months (and years) prior. In March, we covered fugitives being caught within prison and railyard environments; often selecting the same launch spot resulting in their capture.

A great resource the team observed this week was a thorough database of "drone lawsuits and litigations" – an exceptional archive with added statistics captured towards the end. A useful resource and I'm sure the quote "*The DJI Phantom is starting to be like (as common as) the AK-47 of the drone world*" Isn't just one shared by the author.

A key topic of discussion this week was the final issue of the Center for Study of the Drone's Weekly Roundup – an incredible effort by the team at Bard College that have documented, investigated and analysed all things drone and drone security for an incredible eight years. The Center has teased the possibility of a continuation of sorts, so we'll all be paying close attention. With their final release was an update to the Drone Databook – tracking developments in global military drone proliferation; this is included in our publications section.

This week we have had the opportunity to include an intelligence artefact submitted by one of our Notify customers. To that source we thank you for your submission and remind subscribers of the various benefits that come with sharing intelligence with the DroneSec Notify community. Stay safe in these uncertain times and join in the discussion in our slack channel.

- *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. MONTHLY ROLL-UP

As we enter the month of April, Notify features an aggregated summary of drone incidents, types and affected sectors in the past months of 2020 and collated numerical data on drone incidents for the year. Extended analytics with full database-searchable functionality is only offered to our Plus and Premium members, with improvements currently taking place on the platform.

Below you'll find some handy statistics to measure correlation, location and systems involved over data we've collected since January 2020. Anything we've missed? Anything you'd like to see? Drop us a note at info@dronesec.com to get in touch with the team.

In 2020 thus far, four hundred and forty-eight artefacts were recorded which roughly equates to 4.9 drone security incidents/events **per day.** The number of events logged has increased month after month despite the increasing number of regulations set by regulators to dampen drone operations. One reason could be due to the extensive usage of drones worldwide in combating COVID-19. The Chinese government has shown precedence in the effectiveness of drones in disinfecting neighbourhoods and monitoring movement of citizens. Global regulators are also following suit in the utilisation of drones to maintain law and order during the crisis.

Month	Number of Artefacts	Global number of incidents per day	Month-on-month increase
January	135	4.3	N/A
February	139	4.8	4 (2.88%)
March	174	5.6	30 (20.11%)
Total (2020)	448	4.9	N/A

The DroneSec platform tracks incidents, events and these categories/tags allows us to visualise them on a month to month basis. The statistics below are for the month of January and March 2020: Notify release #4 – #16. We see an increase in number of artefacts for Drone Technology due to the increased use of drones during the global COVID-19 movement lockdown and disinfecting of cities.

Category	Number of Artefacts
Featured	19
Cyber and Information Security	10
News and Events	135
Whitepapers and Publications	78
Counter-Drone Systems	51
UTM Systems	17
Drone Technology	63

One key metric we use is priority level – this is explained in our Appendix but means an artefact (determined by category) can change priority based on our matrix. For that reason, it can be insightful to gauge how we align evidence of events to perceived organisational priority and risk. Below you'll find a breakdown of how many artefacts were reported in each priority tier. As with any security threat modelling, it's difficult to ascertain risk without knowing what an organisation deems important in their unique environment. As a company, we try to prioritise specifics (e.g. keywords provided by a customer) over unknowns to filter out noise and ensure notifications do not include 'SPAM'.

March 2020 saw a higher increase in number of P5 artefacts due to the widespread use of drone technology by governments around the world. Drones are utilised to control and restrict movement, spread public message to citizens and to disinfect/sanitise cities.

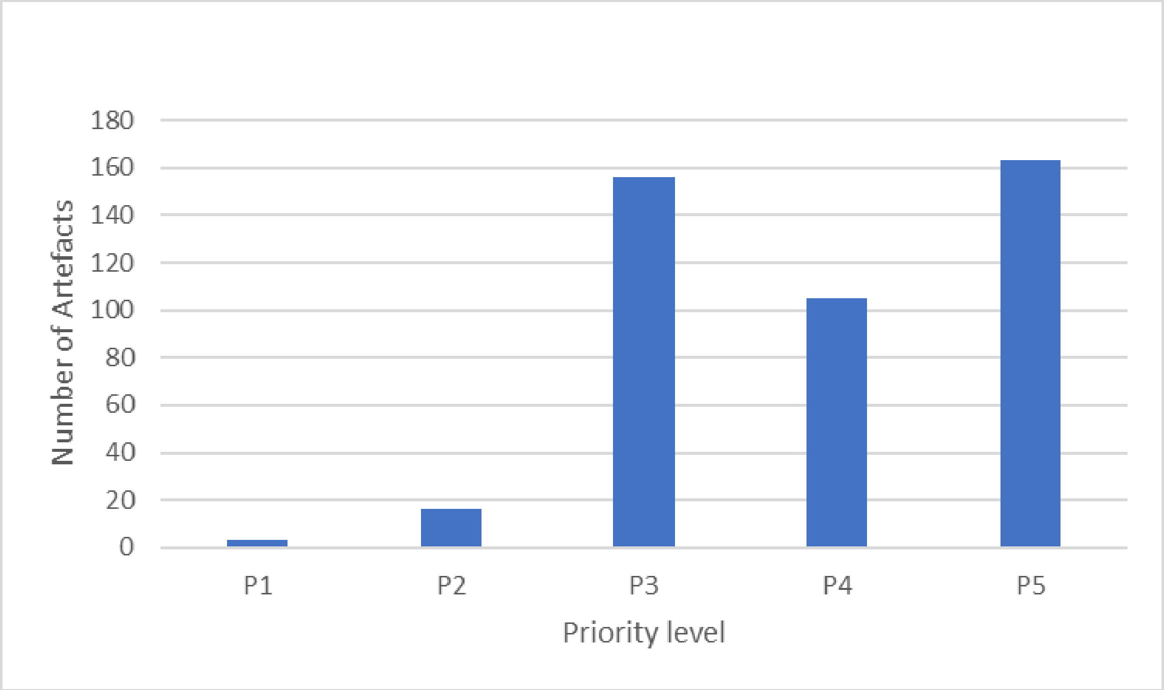


Figure 1: Number of Artefacts by Priority Levels (Since January 2020)

Continuing on below, we've gathered some of the key metrics around specific events and the drones involved. This can help assess historical data and determine if patterns exist amongst similar events.

Since January 2020, we have collated a number of incidents where drones have flouted the laws and we see a majority of them reported in cases of illegal infringements such as trespassing into private property or flying into restricted airspace. However, we also note that drones are utilised quite frequently for vices. Offenders and rogue users have found a new means of transportation for their contraband and without the fear of being caught red handed, they would naturally push their luck and capitalise on the use of these small and stealthy drones. While it is hard to have constant watch protection against illegal drone flights into prohibited areas, DroneSec recommends basic drone detection systems at key installations such as prisons, docks, and power plants to protect facilities and alert security control centres on unauthorised drone activity.

In the month of March 2020, we see continued cases of drone deliveries into restricted areas like prisons and across national borders. However, increasingly in the month of March the perpetrators were caught and offender names logged. Offenders tend to get complacent and reuse the same take-off/landing spots - these can often be the key to apprehension tactics involving rogue drone operators.

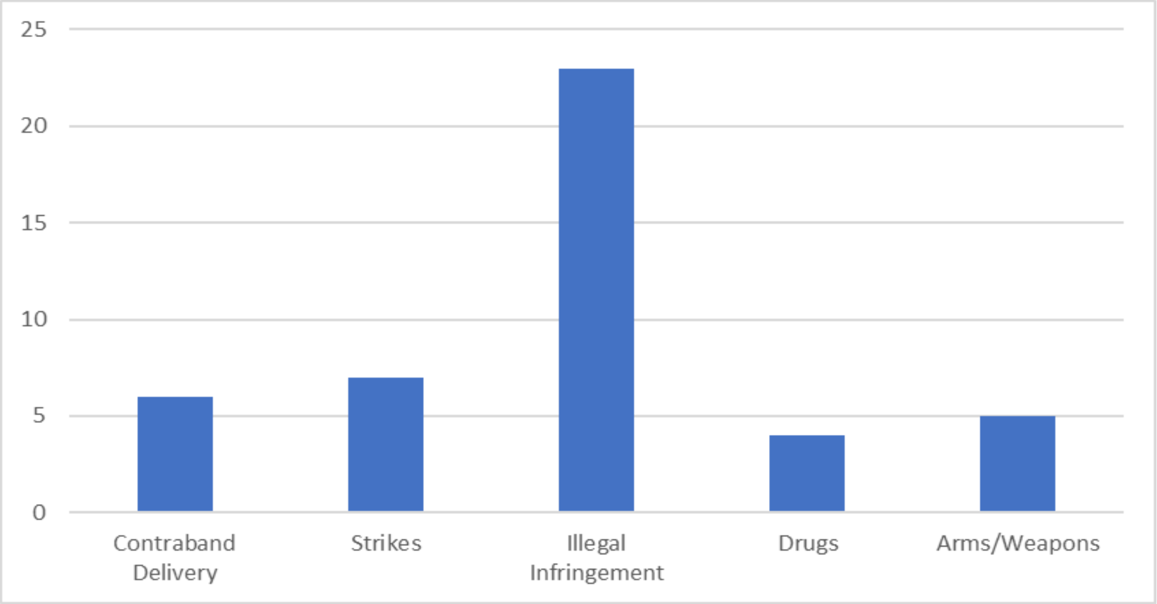


Figure 2: Number of Drones Utilised by Category of Activities (Since January 2020)

DroneSec has also recorded the places and countries where drone incidents have occurred. In March 2020, we see more infringements happening at national borders, neighbourhoods and aerodromes as compared to February 2020. There were several artefacts on near air collision between military aircrafts and drones, blatant infringement of aerodrome, illegal drone deliveries across national borders and terrorist/rogue militas utilising drones for payload-based attacks. Drones are still positioned as a relatively safe method of committing illegal activities, due to the lack of law enforcement strategies and seperation of the operator from their device. Traditional means of securing borders with perimeter fences no longer provide adequate security and air defences against such drones and do not provide a cost effective solution. The current economic ratio of border protection mechanisms costing thousands or millions of dollars against a $500 - $2,000 COTS drone is still very much in the malicious exploiter’s hands.

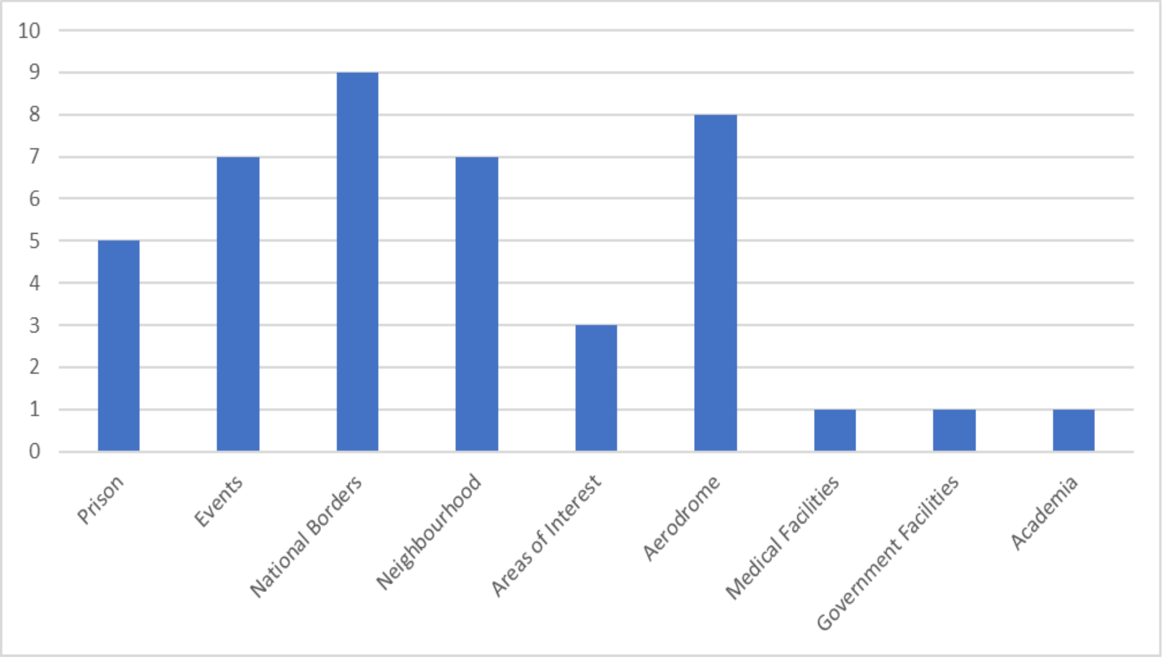


Figure 3: Number of Drone Incidents by Location of Occurrence (since January 2020)

As DroneSec Notify records the number of drone incidents and events happening around the world, we see that the early adopters of drones are mainly from the USA, India, China, UK and Australia. Majority of the artefacts from these countries have seen drones implemented into lifestyles and businesses such as deliveries of supplies, checking on wildlife habitations or used as part of a visual event.

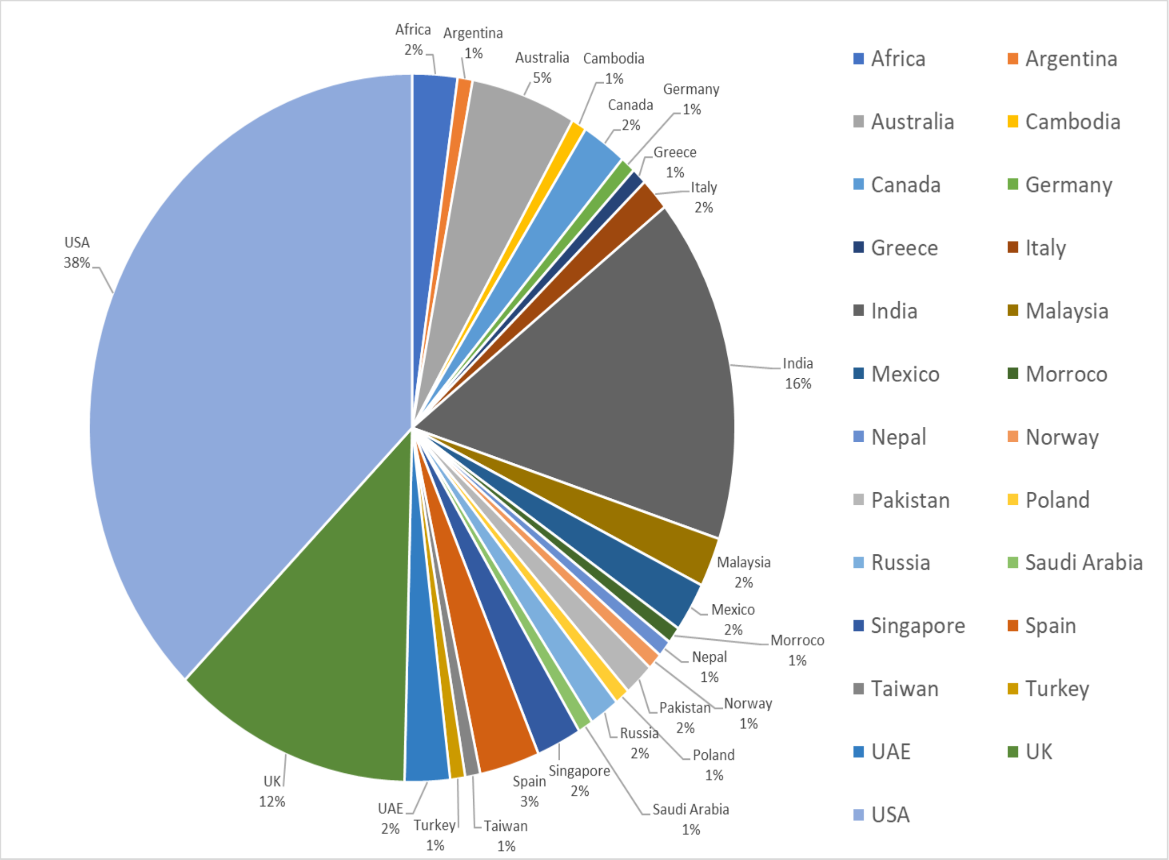


Figure 4: Percentage of Drone Artefacts by Country of Occurrence (Since January 2020)

DroneSec also record the make and model of drones utilised from the artefacts recorded so law enforcement and counter drone industries can prepare themselves with appropriate measures. It is not surprising to see a majority of drones used were from DJI, with a most of these being the Mavic model. A review of law enforcement agencies shows most who possess multiple drones also have a DJI drone to augment their existing fleet.

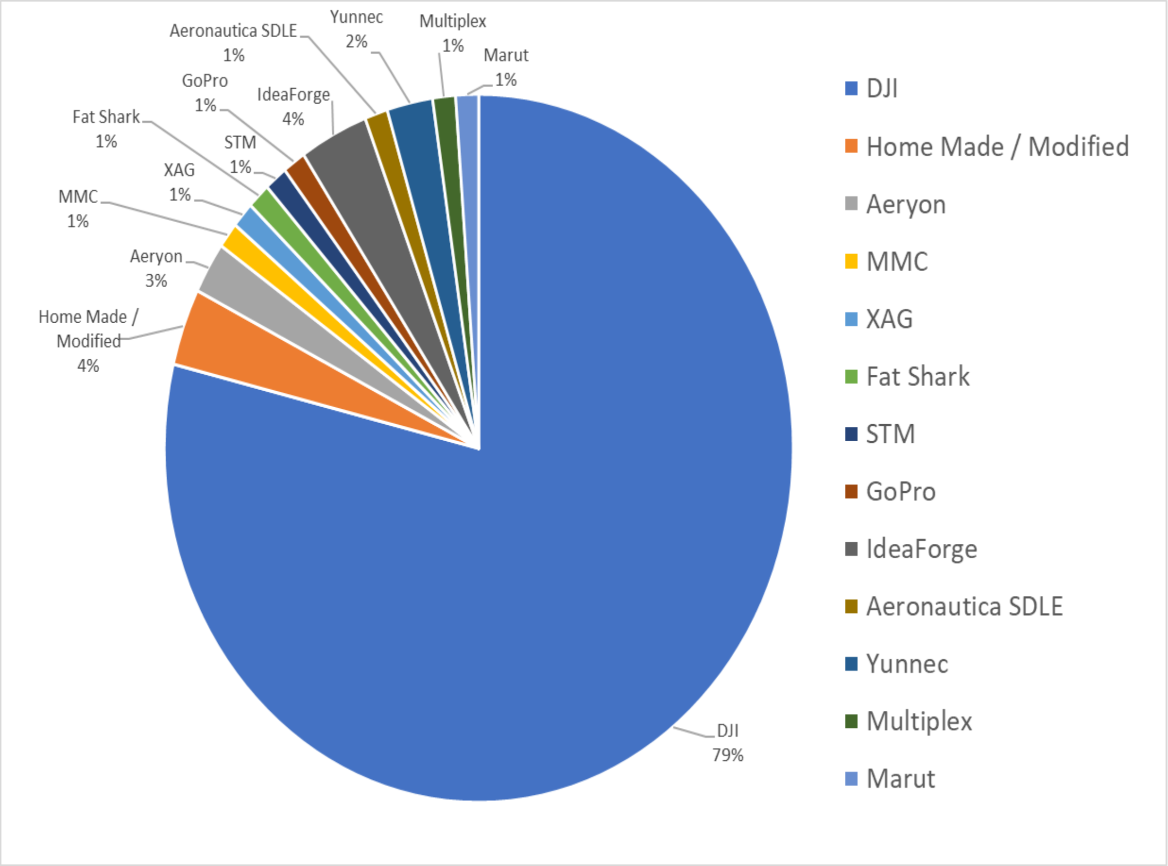


Figure 5: Percentage of Brands of Drones Utilised (Since January 2020)

The DJI Mavic is versatile in many kinds of surveillance operations as it is light weight, fast and portable. It has gained popularity amongst hobbyists, law enforcement, government and security agencies due to its capability in carrying multiple sensor payload (thermal and electro-optic), fast speeds of up to 72km per hour and its small and portable cross-section footprint.

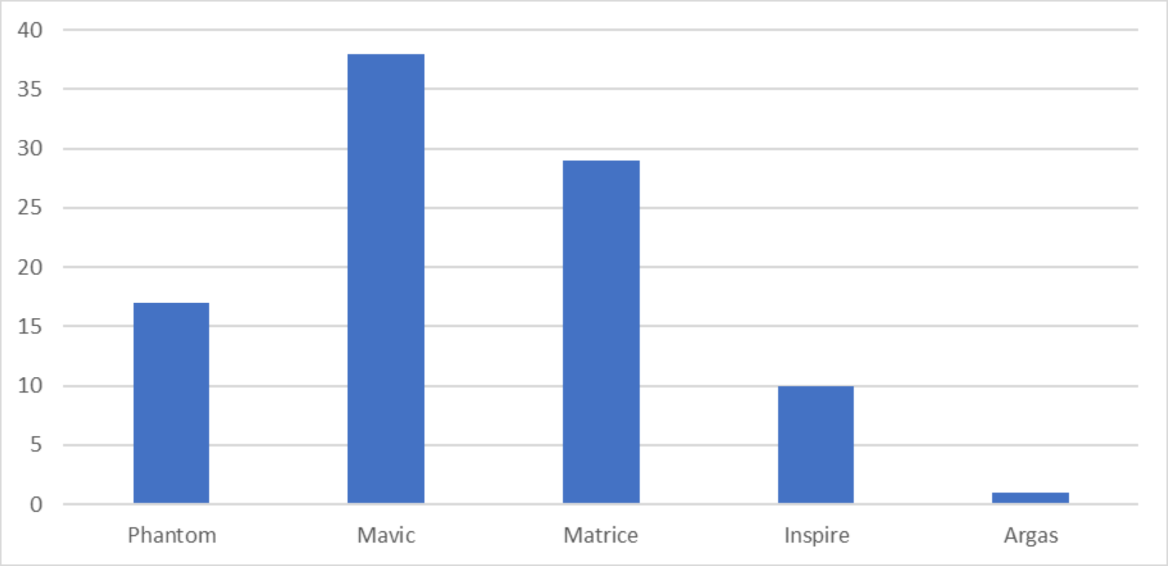


Figure 6: Number of DJI Drones Utilised by Category of DJI Models (Since January 2020)

Interestingly, while the DJI drones are popular amongst security enforcement agencies, law enforcement across the globe have differing preferences on drone acquisition. India prefers the DJI Phantom models and the Indian made Netra and Multiplex drones. The UK and the USA prefer the DJI Mavic and Matrice models, albeit the various restrictions regarding overseas made drones.

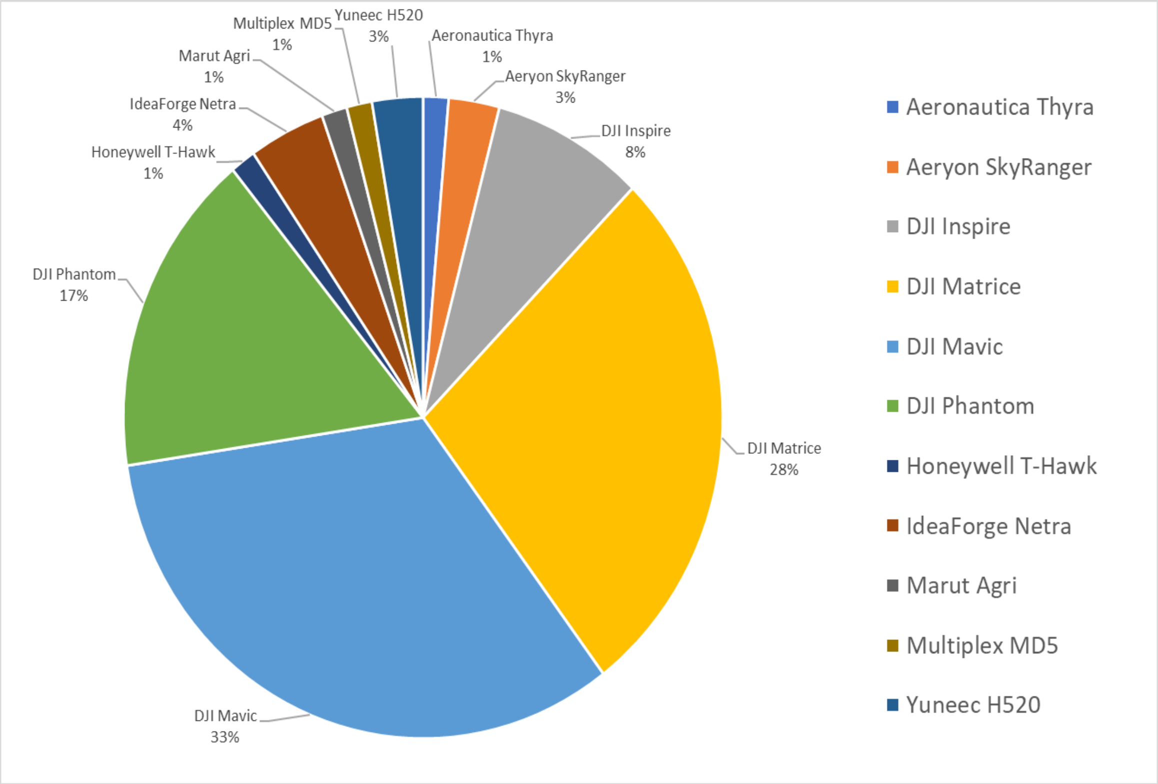


Figure 7: Percentage of Drone Utilised by Enforcement Agencies by Drone Model (Since January 2020)

That concludes our monthly roll up for March. For more advanced statistics like these, get in touch with the team to find out what a Notify PLUS or PREMIUM subscription can offer.

1.3. FEATURED ADVISORIES (P2)

There were no public advisories sent to Notify subscribers this week.

1.4. NEWS AND EVENTS (P3)

Japanese Police arrested 115 offenders in 2019 for illegal and unauthorised drone flights

https://www.japantimes.co.jp/news/2020/03/26/national/crime-legal/drone-flights-2019/#.Xnx0Fm5uIhk

Israeli Defence Force shoots down small Hezbollah drone infringing airspace

https://hamodia.com/2020/03/26/idf-shoots-hezbollah-drone/

Derbyshire Police, UK, dye lagoon black to tourist prevent drone flights

https://nationalpost.com/pmn/health-pmn/black-dye-and-drones-english-police-bemuse-public-with-coronavirus-response-2

Arab coalition takes down three rogue drones targeting civilians in Saudi Arabia

https://www.reuters.com/article/us-saudi-houthis-drones-idUSKBN21D3UG

U.S. Marine Corps to double UAS squadrons in line with National Defense Strategy

https://seapowermagazine.org/marine-corps-to-double-uas-squadrons-reduce-rotary-squadrons-by-2030/

1.5. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P3)

Center for Study of the Drone: Drone Databook (March 2020 Update)

https://dronecenter.bard.edu/projects/drone-proliferation/drone-databook-update-march-2020/

https://dronecenter.bard.edu/files/2020/03/CSD-Databook-Update-March-2020.pdf

BVLOS licensing system for drones to be established in Japan

https://mainichi.jp/english/articles/20200330/p2g/00m/0na/058000c

Civil Authority Malaysia: all drone operators to apply for permits for COVID usage

https://www.malaymail.com/news/malaysia/2020/03/27/any-parties-using-drones-for-covid-19-surveillance-must-still-obtain-caam-a/1850743

Hackin9: Drone Hacking, Exploitation and Vulnerabilities (PDF available to Notify Customers)

https://hakin9.org/product/drone-hacking-exploitation-and-vulnerabilities/

HackMiami: Drone Security Defending, Hacking and Hardening (Henry Secove)

https://www.youtube.com/watch?v=-6jHh_YUNvQ

https://drive.google.com/file/d/1LtaqBFeMM028IZ5xEayF_iGjKGWhZ38v/view

Drone Lawsuits and Litigation Database

https://jrupprechtlaw.com/drone-lawsuits-litigation

1.6. COUNTER-DRONE SYSTEMS (P4)

Four organisations shortlisted for Australia's project LAND 129 phase tender

https://aaus.org.au/l129-3-industry-participation/

Pentagon's top weapons buyer directs army to focus on counter-drone effort

https://www.msn.com/en-us/news/world/us-sees-war-zone-drones-as-new-improvised-explosive-devices/ar-BB110uQb?utm_source=Sailthru&utm_medium=email&utm_campaign=EBB%2003.11.20&utm_term=Editorial%20-%20Military%20-%20Early%20Bird%20Brief

1.7. UTM SYSTEMS (P4)

European drone-airspace management service launched

https://www.gpsworld.com/european-drone-airspace-integration-project-kicks-off/

Merging of Air Traffic Control and UAS Traffic Management systems (Commentary)

https://www.commercialuavnews.com/infrastructure/is-this-the-right-time-to-test-the-merging-of-atc-and-utm

1.8. DRONE TECHNOLOGY (P5)

Australian researchers and Draganfly develop drone and sensor suite to detect people with infectious respiratory conditions

https://indaily.com.au/news/science-and-tech/2020/03/26/pandemic-drone-could-detect-virus-symptoms-in-crowds/

Melbourne based Swoop Aero pioneers international drone delivery in Africa

https://www.afr.com/technology/melbourne-startup-swoop-aero-wins-first-contract-to-deliver-vaccines-via-drones-20181023-h16z7m

First BVLOS drone flight for Canada approved with onboard avoidance system

https://finance.yahoo.com/news/first-approval-beyond-visual-line-100200579.html

UPS partners with Wingcopter to develop high speed delivery drones of 150mph

https://www.dailymail.co.uk/sciencetech/article-8153261/UPS-developing-fleet-high-speed-delivery-drones-capable-speeds-150mph.html

Pune police, India, uses facial recognition tech on drones during virus lockdown

https://indianexpress.com/article/cities/pune/pune-police-use-drones-to-track-home-quarantined-persons-6337618/

Mayor of Messina, Italy, uses Phantom 4 drones to curse at citizens to stay home

https://www.5why.com.au/an-italian-mayor-is-getting-drones-to-literally-swear-at-people-who-ignore-coronavirus-warnings/

Indian government engages Garuda Aerospace for disinfectant spraying

https://kalingatv.com/nation/drones-to-power-fight-against-coronavirus-in-chhattisgarh/

Derbyshire Police, UK, uses drones to shame citizens flouting travel restriction order

https://www.theguardian.com/world/video/2020/mar/26/police-drone-video-shames-people-using-national-park-during-uk-lockdown-video

Elche Police, Spain, enrols DJI Mavic to monitor beaches and parks to enforce lockdown

https://www.costablancapeople.com/news/elche-police-will-monitor-beaches-and-parks-with-drones-this-weekend/

Dubai Government uses DJI Matrice to aid in disinfecting city from COVID-19

https://www.the961.com/dubai-is-using-drones-to-disinfect-all-the-city/

Kerala Police, India, uses Phantom 4 to fine citizens who leave homes without valid reason

https://telanganatoday.com/kerala-police-deploy-drones-to-book-lockdown-violators

Nagaland government, India, spreads COVID awareness rules via drones

https://www.eastmojo.com/coronavirus-updates/2020/03/27/nagaland-govt-uses-drones-in-kohima-to-spread-covid-19-awareness

Welsh council, UK, deploys DJI Mavic to disperse groups of people during lockdown

https://www.walesonline.co.uk/news/wales-news/drones-lockdown-coronavirus-wales-council-17989877

Kauai PD, US, secures more drones for natural disasters and search and rescue operations

https://www.thegardenisland.com/2020/03/27/hawaii-news/kpd-prepping-more-drone-use/

Al-Qassim, Saudi Arabia, utilises drones with thermal scanners to monitor body temperature

http://www.saudigazette.com.sa/article/591305

Ahmedabad police, India, hires drone operators to keep watch on citizen's movement

https://timesofindia.indiatimes.com/city/ahmedabad/lockdown-in-ahmedabad-police-use-drone-to-restrict-peoples-movement/articleshow/74853136.cms

Northamptonshire will be using drones to spread public information messages

https://www.northamptonchron.co.uk/health/coronavirus/drones-may-blare-out-public-information-messages-northamptonshire-says-chief-constable-2504505

DJI Mavic and Matrice deployed to enforce social distancing by Western Australia Police

https://www.news.com.au/national/drones-deployed-to-police-social-distancing-in-wa/video/ddae062ff7dc9f5bd784fefea8e8be4b

6 Alpha 800 and Multiplex MD10 drones to disinfect Bengaluru city

https://www.wionews.com/india-news/bengaluru-uses-drones-to-disinfect-the-city-289682

Ilocos Norte, Philippines, on extended quarantine uses drones to disinfect city

https://northluzon.politics.com.ph/ilocos-norte-town-uses-drones-to-disinfect-communities/

1.9. INFORMATIONAL (P5)

Drone and Data Academy set up by UNICEF in Africa to teach skills on drone flying

https://www.unicef.org/malawi/african-drone-and-data-academy-malawi

Sussex Police, UK, deploy drone to look for missing teenager

https://www.brightonandhovenews.org/2020/03/29/police-helicopter-and-drones-used-in-search-for-missing-saltdean-teenager/

Dark side of aerial drones (commentary)

https://www.techtimes.com/articles/248473/20200331/aerial-drones-innovative-until-privacy-security-risk-heres-dark-side.htm

Russian Altius attack drone bypasses air defences without human interaction

https://www.armyrecognition.com/weapons_defence_industry_military_technology_uk/russian_altius_attack_drone_to_operate_in_autonomous_regime.html

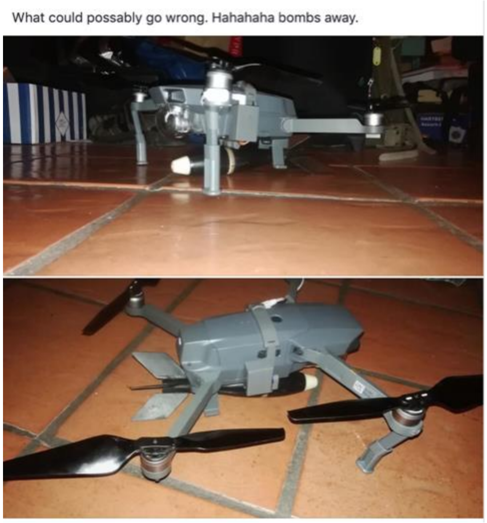
Mountain Home 366th Security Forces Squadron test new Gen 4 InstantEye Mk-3 drone

https://www.youtube.com/watch?v=zTe5hQFqO0E

1.10. SOCIAL (P3)

Modding of DJI Mavic to carry payloads

Taken from a social media group, the drone (DJI Mavic) was observed to have been modified to be able to carry a small payload representing an explosive.

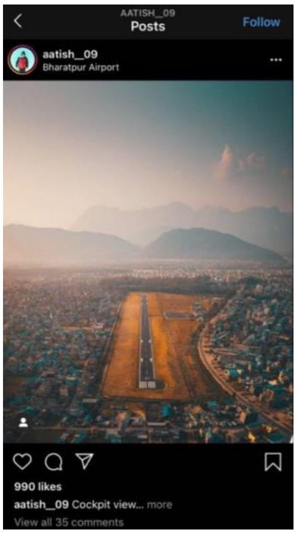


What could possably go wrong. Hahahaha bombs away.

Figure 8 - Anonymous DroneSec Notify Customer Submission

Social media posts on photos of approach path of commercial airport taken by drones

Images and accounts were taken down at time of posting. The author flew his DJI Mavic 2 Pro over Bharatpur airport along the approach path of incoming civil aircraft to capture a shot of the airfield. The airport was stated to be closed at this time due to COVID-19.

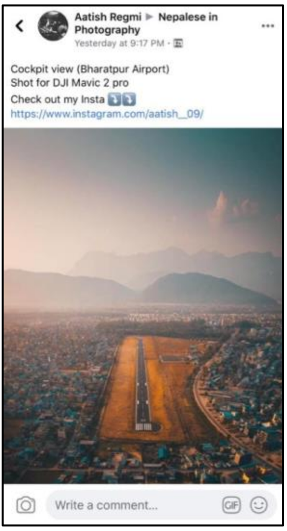


aatish_09
Bharatpur Airport

990 likes

aatish_09 Cockpit view... more

View all 35 comments

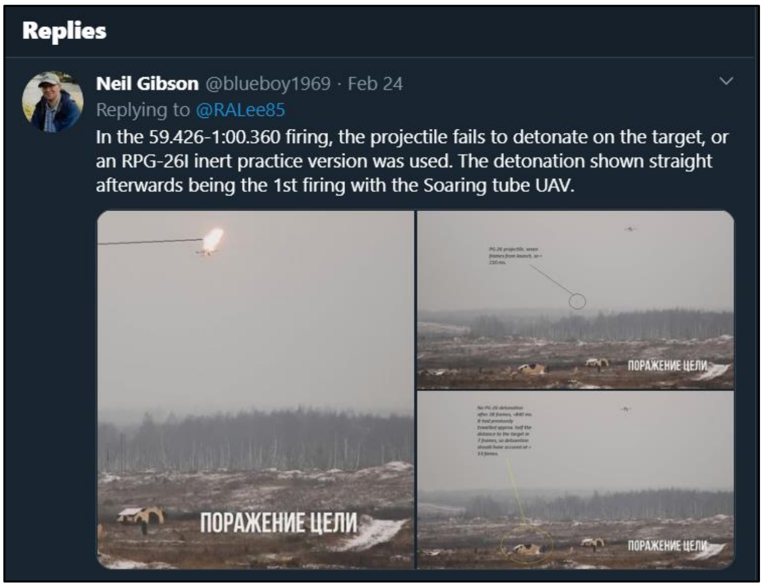

Aatish Regmi ▶ Nepalese in Photography
Yesterday at 9:17 PM ·

Cockpit view (Bharatpur Airport)
Shot for DJI Mavic 2 pro
Check out my Insta ⤵️⤵️
https://www.instagram.com/aatish_09/

Belarusian Kvadro-1400 UAV equipped with two RPG-26 rocket launchers video analysis

Source: https://twitter.com/RALee85/status/1231726835861458944?s=20

Reply: https://twitter.com/blueboy1969/status/1231875429633581057?s=20


Replies

Neil Gibson @blueboy1969 · Feb 24
Replying to @RALee85
In the 59.426-1:00.360 firing, the projectile fails to detonate on the target, or an RPG-26I inert practice version was used. The detonation shown straight afterwards being the 1st firing with the Soaring tube UAV.

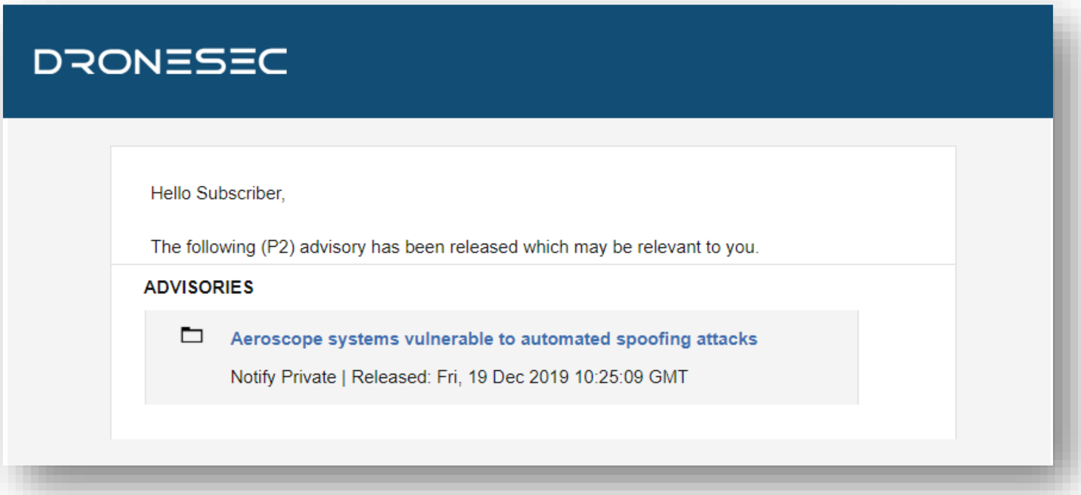
APPENDIX A: THREAT NOTIFICATION MATRIX

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 9 - 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.