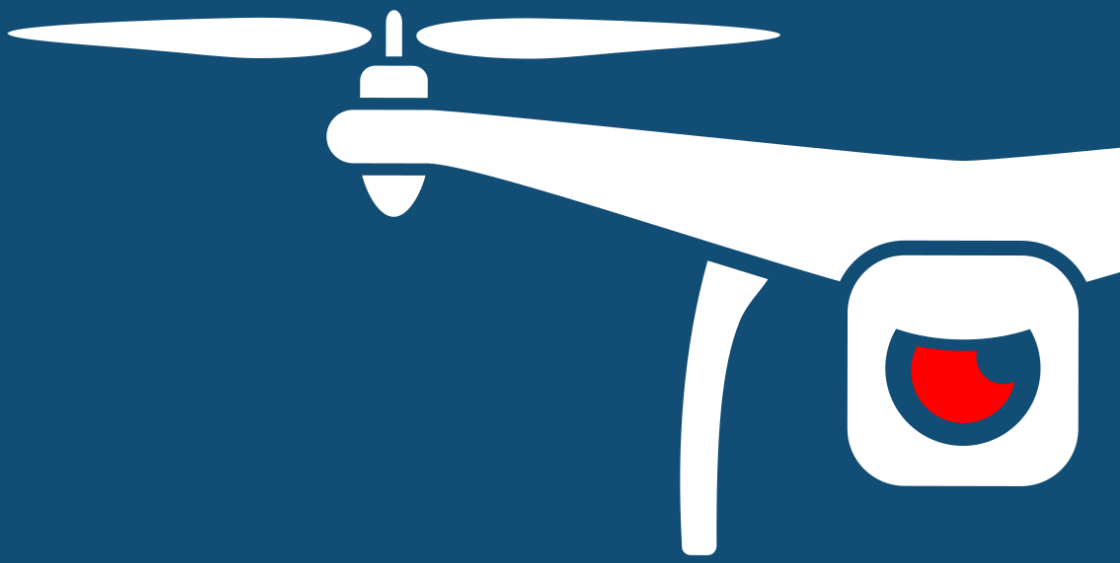
DRONE SEC
A Privasec COMPANY

NOTIFY ISSUE #8

WEEKLY THREAT INTELLIGENCE

05 February 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

The month of January is gone and our roll-up is here. We've provided some statistics to give a snapshot of the month gone by and as usual, will continue to compare each month forward.

A special nod to our readers – we've had some really constructive input in our methodology and roadmap in the last few weeks which will continue to shape Notify in the months forward. A special thanks to Kevin Manderson from Telstra (Threat Intelligence and Incident Response team), and David Kovar from URSA (specialist UAV Forensics and Analytics firm) for their contributions.

The first ever DroneSec podcast recording was actually on the Randy Goers "Drone Radio Show" – in fact, it was likely the first drone 'security' podcast recording during that time. Since then, Randy has interviewed countless drone security and counter-drone episodes. Another one just came out this week on RF as a detection mechanism; it's mentioned in this issue below, so go check it out; Randy's podcast has a special place in the DroneSec team's heart.

We will be operating on a different time zone next week as the bulk of the team is in Singapore for the Global Drone Security Network, Cyber Attack conference and Singapore Air Show. Notify public will be released as usual on Wednesday, maybe a few hours difference.

- *Mike Monnik, DroneSec CTO*

TABLE OF **CONTENTS**

1. Threat intelligence ---- 5
1.1. Introduction ---- 5
1.2. Monthly Roll-up ---- 6
1.3. Featured Advisories ---- 10
1.4. News and Events (P3) ---- 11
1.5. Whitepapers, Publications & Regulations (P3) ---- 12
1.6. Counter-Drone Systems (P4) ---- 13
1.7. Informational (P5) ---- 13
APPENDIX A: Threat Notification Matrix ---- 14
A.1. Objectives ---- 14
APPENDIX B: Sources & Limitations ---- 18
B.1. Intelligence sources ---- 18
B.2. Limitations ---- 19

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 new month, Notify features a aggregated summary of drone incidents, types and affected sectors in the past month(s) (January 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 constant 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 for the January period. 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.

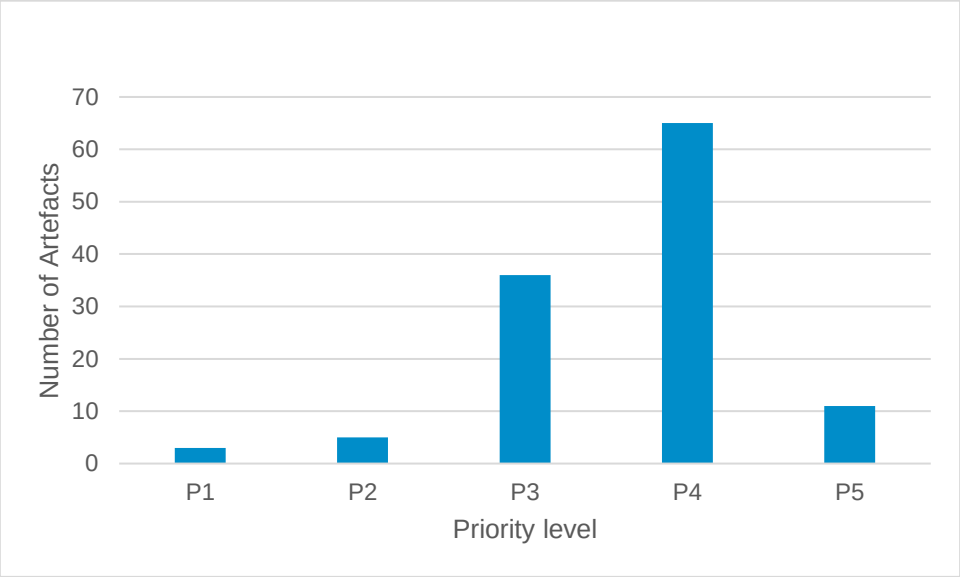
Month	Number of Artefacts	Global number of incidents per day
January	135	4.3

Kicking off 2020, one-hundred and thirty-five artefacts which roughly equates to 4.3 drone security incidents/events **per day.** Impressive (or slightly worrying), considering the young age of drone technology and pales in comparison to the *billions* of computer-security incidents we see on a global scale today. We're hoping drone security won't get to that milestone, but we're preparing for it in case.

The DroneSec platform tracks incidents, their categories/tags and allows us to visualise then on a month to month basis. The statistics below are for the month of January only: release #4 – #7.

Category	Number of Artefacts
Featured	5
Cyber and Information Security	7
News and Events	65
Counter-Drone Systems	18
Whitepapers and Publications	27
UTM Systems	5
Drone Technology	8

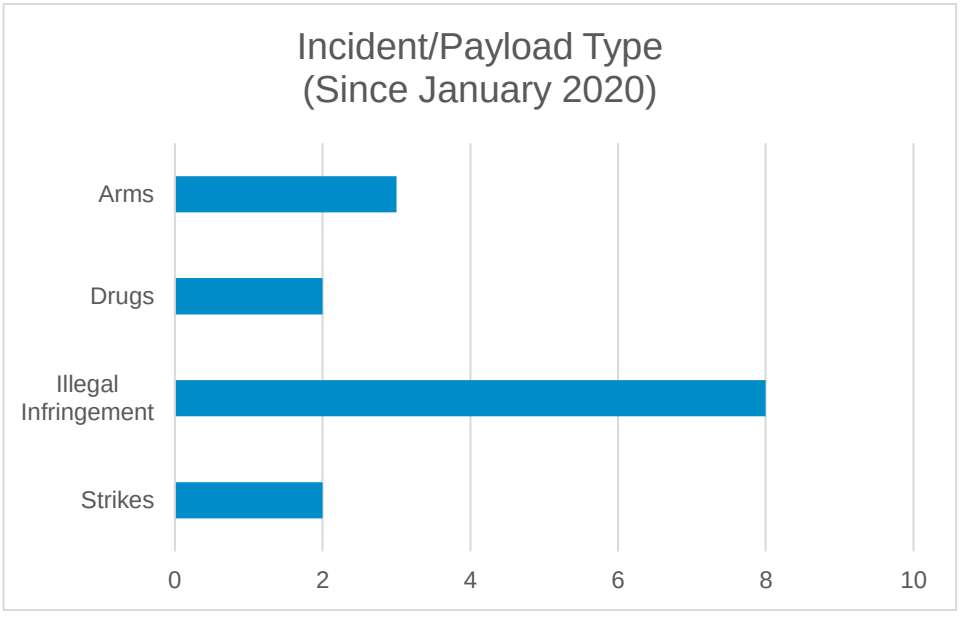
One key metric we use is priority level – this is explained in our Appendix but means an artefact (determined by category) can change priority based on our matrix. For that reason, it can be insightful to gauge how we align evidence of events to perceived organisational priority and risk. Below you'll 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' (e.g. P4's).

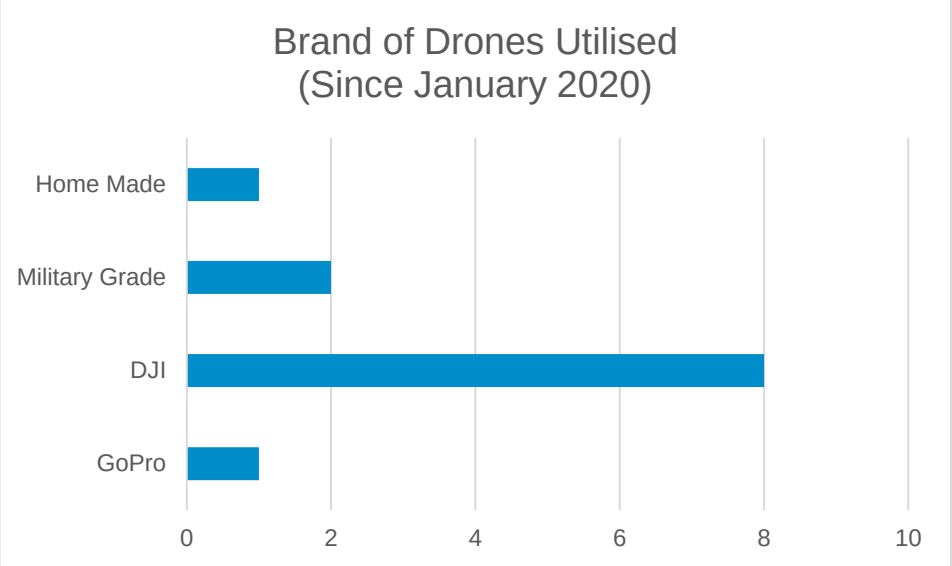


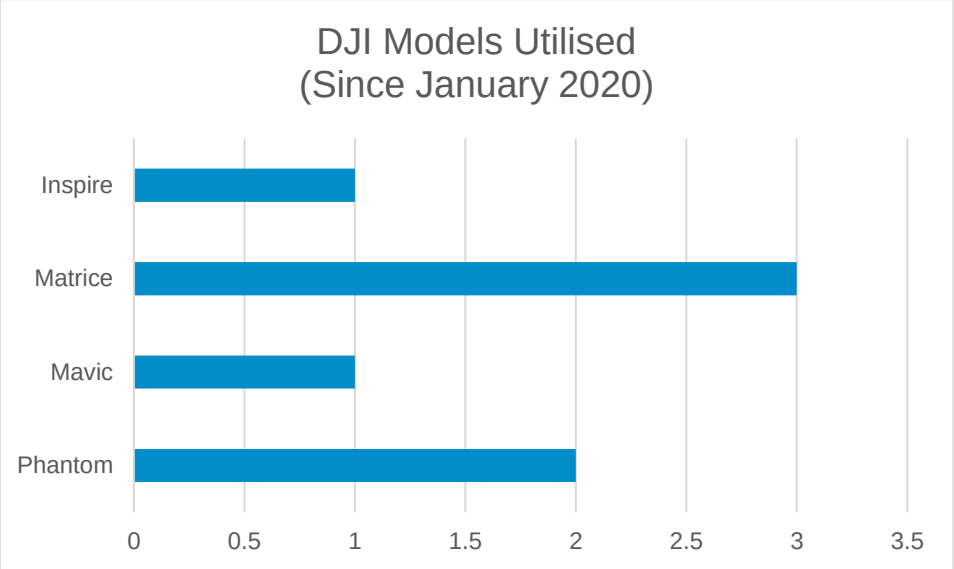
Continuing on below, we've gathered some of the key metrics around specific events and the drones involved. This can help assess historical data and determine if patterns exist amongst similar events.

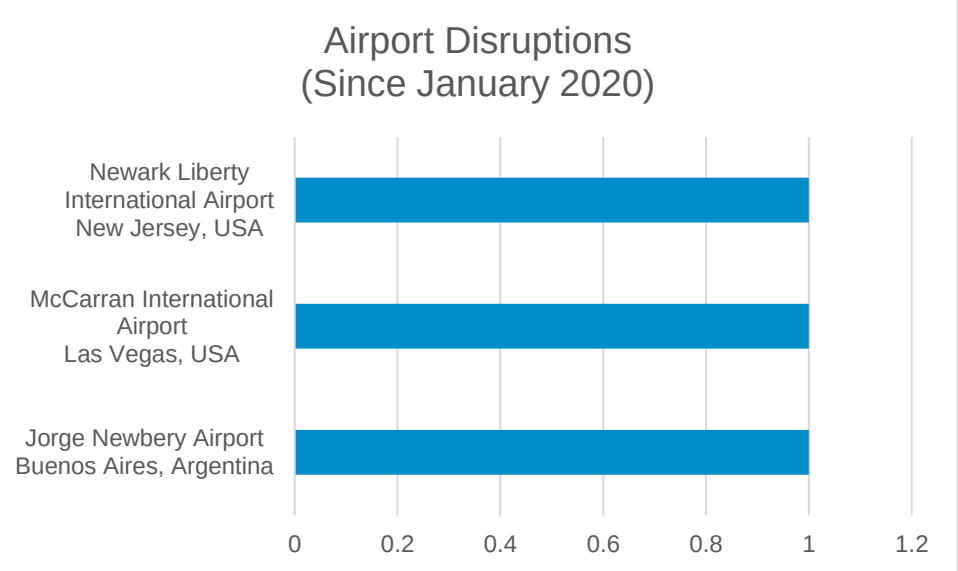
Drone Incident	Location	Type of UAS Used	Organisation	Notify Issue
Drone strike kills Iranian elite force commander, Qasem Soleimani	Baghdad International Airport, Baghdad	MQ-9 Reaper	USAF	#4
Drone drops meth over Australian prison	Capricornia Correctional Centre, Queensland, Australia	Not mentioned	Unknown, possibly cartels	#4
Drone collision with airliner	Jorge Newbery Airport, Buenos Aires	Not mentioned	Unknown, possibly personal	#4
Malfunctioned drone lands in operational airport	McCarran International Airport, Las Vegas	DJI Phantom 3	Personal	#4
Unauthorised drone flight during FA-18 flight demo	Newcastle, Australia	Not mentioned	Unknown, possibly personal	#4
Drone grounded due lack of software update	Nil	GoPro Karma	Nil	#4
Drone experienced technical failure when in contact with moisture	Nil	DJI Matrice 200/210	Nil	#5
Drone sent to Syria terror group, Al-Qaida	Turkey	DJI Phantom 3	Al-Qaida	#5

Drones used to smuggle drugs and arms consignment across borders	India - Pakistan	DJI Inspire 02 DJI Matrice 600	'Khalistan Zindabad Force' terrorists	#5
Hunters arrested for using drones for scouting animals	Morgantown, West Virginia, USA	DJI Mavic Mini	Personal	#6
Drones carrying projectiles shot down by military AA systems	Latakia, Syria	Self-made	Levant Liberation Board, branch of al-Qaida	#6
Drone infringement over MOD	Telford, UK	Not mentioned	Unknown, possibly personal	#6
Chinese UAV crash lands in Cambodia	Cambodia	Harbin BZK-005 / Cai Hong-92A	Unknown	#6
FAA closes airspace around basketball legend's helicopter crash	Calabasas, California, USA	Not mentioned	Unknown, possibly personal	#7
Drone activity halts air traffic at international airport	Newark Liberty International Airport, New Jersey, USA	Not mentioned	Unknown, possibly personal	#7
Woman stalked by drone for hours	Maine, USA	Not mentioned	Unknown, possibly personal	#7
Taliban seized weaponised drone from Afghan security forces	Garamsir, Afghanistan	DJI Matrice 210	Afghan security forces	#7









That concludes our monthly roll up for January. 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

Featured Article	Tags
Drone operations heavily utilised by Chinese authorities to control virus outbreak	Drones, All Sectors, Safety

Overview

Following the Coronavirus outbreak in China, authorities have been reported to be using drones to ensure citizens are staying indoors and away from public gatherings. They have been used to publicly warn citizens to wear masks outdoors via remote-voice megaphones attached to drones. Other uses include dispersing disinfectants in villages, conducting temperature checks, lighting up building sites and management of waste disposals. All imagery was reported by a Chinese state-run media agency.

References:

- https://www.abacusnews.com/tech/coronavirus-spreads-chinese-drones-drop-disinfectant-and-disperse-public-gatherings/article/3048687
- https://www.youtube.com/watch?time_continue=104&v=8NMqSWZH_k8&feature=emb_logo

Featured Article	Tags
Russian airbase uses 'electronic warfare' measures to intercept and disable illegal drones	Drones, Airport, CUAS, Cyber Security, Government

Overview

Reports emerged from Moscow revealing that multiple drones were launched from the Idlib de-escalation zone and targeted the Russian Hmeimim airbase in Syria. The drones were launched from 'illegal armed units' and detected by the airbase's airspace control unit.

DroneSec Analysis

The interesting statement however, is that from Major General Yuri Borenkov, who explained that 'electronic warfare' measure at the airbase intercepted and disabled the UAV's by disrupting their controls systems. It does not mention the type, size or navigational capabilities of the drones. DroneSec were unable to locate information suggesting any current commercial counter-drone vendor was responsible for the electronic warfare installation that was suggested to have defeated the drones.

References:

- https://sputniknews.com/middleeast/202002021078207158-drones-downed-near-russias-hmeimim-launched-from-idlib-zone/

Featured Article	Tags
U.S. Interior Department moves from drone 'pause' to 'grounding' amid potential cybersecurity risk	Cyber Security, Safety, Government, Regulation , Critical Infrastructure and Security

Overview

Drawing reference to Article 7 of China's 2017 National Intelligence Law in play, the U.S. Department of Interior (DOI) is citing that foreign-made drones and its components could have potential cybersecurity risk. An example of this risk is alleviated in Article 7 of the abovementioned law which requires Chinese companies to comply and provide imagery data to the Chinese government. The DJI Matrice 600 Pro and DJI Mavic Pro models are the main drones used by U.S. government agencies including emergency services. A total of 10,432

drone flights were conduct in 2018, building up a sizeable amount of imagery data on the United States. Although, the move to ground all foreign-made drones would be in effect until revoked, drone operations for emergency purposes will still be approved.

DJI has claimed the move to be politically motivated despite their efforts working with the government to alleviate security concerns about its drones. With most of the world's electronic components being made in China, DJI rebutted that U.S. government are currently using laptops, tables, smartphones containing Chinese components within the agencies.

DroneSec Analysis

Whilst most components are made in China, there are many necessary measures to ensure that data is secure and sovereign – both in the hardware and software. Highly classified data should never be subjected to internet-connected devices without independent analysis and assessment. In any case utilising drones for government operations, the drone, it's hardware, software and associated devices should function behind a standalone intranet or private network to alleviate the possibility of data being compromised. Likewise, personal data and photos should not be stored in publicly accessible cloud infrastructure.

References:

- https://www.npr.org/2020/01/29/800890201/interior-department-grounds-all-of-its-drones-citing-cybersecurity-other-concern
- https://content.dji.com/how-the-us-department-of-the-interiors-new-drone-policy-hurts-america/
- https://www.reddit.com/r/drones/comments/exh50h/dji_drones_a_threat_to_us/ (Commentary)

1.4. NEWS AND EVENTS (P3)

Drone presence in Madrid airport delays flights and shuts down airport

https://www.rt.com/news/479959-madrid-barajas-airport-drones-closure/

https://abcnews.go.com/Business/wireStory/drone-sighting-disrupts-air-traffic-madrid-airport-68720877

Yemen government shoots down Houthi rebel group drone hovering over military sites

www.china.org.cn/world/Off_the_Wire/2020-02/02/content_75666529.htm

Man charged for flying drone in restricted air space during Super Bowl week

https://www.nytimes.com/aponline/2020/01/31/us/ap-us-fbn-super-bowl-drone-arrest.html

U.S. confirms strikes against terrorist leader, Qassim al-Rimi, head of Al-Qaeda

https://foreignpolicy.com/2020/02/03/al-qaeda-leader-yemen-believed-killed-c-i-a-drone-strike-arabian-peninsula-security-brief/

Illegal import of 22 Chinese made drones to India seized

https://timesofindia.indiatimes.com/city/mumbai/no-bank-records-of-22-imported-drone-sales/articleshow/73691600.cms

Charges laid against drone operators, inmates for contraband delivery to Collins Bay prison

https://www.thewhig.com/news/local-news/csc-opp-announce-drone-related-arrests-charges

U.S. drones off Syrian coast shot down by Russian Defence Systems

https://www.almasdarnews.com/article/russian-military-may-have-shot-down-us-drones-off-the-syrian-coast-media/

Low flying drone nearly hits Arizona police officer on motorcycle

https://www.azfamily.com/news/drone-nearly-hits-tempe-oolice-officer-on-motorcycle/article_a9c2e9ce-47ac-11ea-96a2-1701e06ec4ba.html

1.5. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P3)

Drone Licensing Rules for Kenya

Previously, the Kenya Department of Defence was the final approving authority for drone licensing after the Kenya Civil Aviation Authority, however, with the new revised draft regulation, drone operators may be applying directly to one inter-ministerial agency instead of multiple. The new draft regulation will also be issue drone operation permits based on security risk instead of weight and use, which considers the applicant's civil or criminal background. In addition, ownership of drone is also not transferrable unless approved by the authority.

https://www.standardmedia.co.ke/article/2001357921/kdf-to-lose-drone-licensing-powers-in-new-proposals

FAA announces Type Certification for drones, requests for comments

The Federal Aviation Authority proposed that some drones are classified as a 'special class' of drone and may require a type certification before operators can fly the drones. The proposed rule establishes the airworthiness criteria of such drone to ensure safe operation and compliance to existing regulations. The proposal is open for comments till March 4, 2020.

https://www.federalregister.gov/documents/2020/02/03/2020-01877/type-certification-of-unmanned-aircraft-systems

https://www.suasnews.com/2020/02/type-certification-of-unmanned-aircraft-systems-a-proposed-rule-by-the-faa/

EU National Aviation Authorities extend collaboration in implementing drone regulations

https://www.unmannedairspace.info/uncategorized/eu-national-aviation-authorities-extend-collaboration-in-implementing-drone-regulations/

https://uvs-international.org/wp-content/uploads/2020/01/Madrid-Declaration-of-Intent_Final_190124_B_TR.pdf

Japan to reform drone laws with focus on domestic industry and 'secure information system'

https://www.unmannedairspace.info/emerging-regulations/japan-reforms-drone-laws-with-focus-on-domestic-industry/

Exploiting multi-vendor vulnerabilities as backdoors to counter the threat of rogue small UAS

https://dl.acm.org/doi/10.1145/3215466.3215467 (PDF available to Notify customers)

Analysis of the GPS spoofing vulnerability in the 3DR solo drone

https://ieeexplore.ieee.org/document/8691741/ (PDF available to Notify customers)

How to govern the non-cooperative amateur drones?

https://ieeexplore.ieee.org/document/8648452/ (PDF available to Notify customers)

1.6. COUNTER-DRONE SYSTEMS (P4)

Fortem Technologies announces TrueView R30 radar for drone detection and threat assessments

http://www.prnewswire.com/news-releases/fortem-technologies-announces-complete-end-to-end-c-uas-solution-300997194.html

New joint research between Britain radar company and drone researcher to track drone in 3D

https://dronelife.com/2020/02/03/new-radar-system-can-track-drones-in-3d/

Israeli Drone Guard counter-drone system tested at multiple airports in North, South America

https://en.globes.co.il/en/article-iai-elta-successfully-tests-airport-anti-drone-system-1001316366

1.7. INFORMATIONAL (P5)

U.S. Defense Innovation Unit (DIU) focuses on net-grabbing CUAS for soft-downing of drones

https://www.defenseone.com/technology/2020/02/pentagon-spending-millions-dollars-hunter-drones-nets/162835/

Cleveland Police to use drones to fight crime and protect public through tracking and FLIR

https://www.hartlepoolmail.co.uk/news/crime/cleveland-police-launch-their-first-aerial-drones-help-fight-crime-and-protect-public-1379535

English Police deploy drones with thermal imaging to deter night-time car thefts

https://www.lancasterguardian.co.uk/news/crime/police-deploy-night-drone-halton-after-thieves-attempt-cut-catalytic-converter-1383479

Ontario Police deploys drones to detect, monitor and enforce cannabis distance regulations

https://www.thegrowthop.com/cannabis-news/cops-and-robbers-ontario-county-enlists-drones-in-fight-against-illicit-cannabis

Pennsylvania State officials warn public of drone interruptions to emergency vehicles

https://www.abc27.com/news/local/state-officials-warn-of-drone-use-during-emergency-situations/

Woman calls Police over rogue operator flying drone outside window in Port Dover, Canada

https://kitchener.ctvnews.ca/woman-changing-in-her-bedroom-sees-drone-hovering-outside-her-window-1.4785322

Commentary: Data Security is the critical foundation for the success of remote ID

https://www.unmannedairspace.info/commentary/data-security-the-critical-foundation-of-remote-id/

Secure flight private network tested for IoT-connected sensitive drone operations

https://finance.yahoo.com/news/syniverse-ge-aviation-airxos-build-130500623.html?guccounter=1

Ukrainian quadcopter built to withstand electromagnetic spectrum interference

https://www.c4isrnet.com/unmanned/2020/01/29/new-savior-drone-is-read-for-the-trenches-of-the-2020s/

Podcast interview: Are RF-based detection systems effective in stopping drones

http://droneradioshow.com/are-rf-detection-systems-effective-in-stopping-drones/

APPENDIX A: THREAT NOTIFICATION MATRIX

A.1. OBJECTIVES

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

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

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

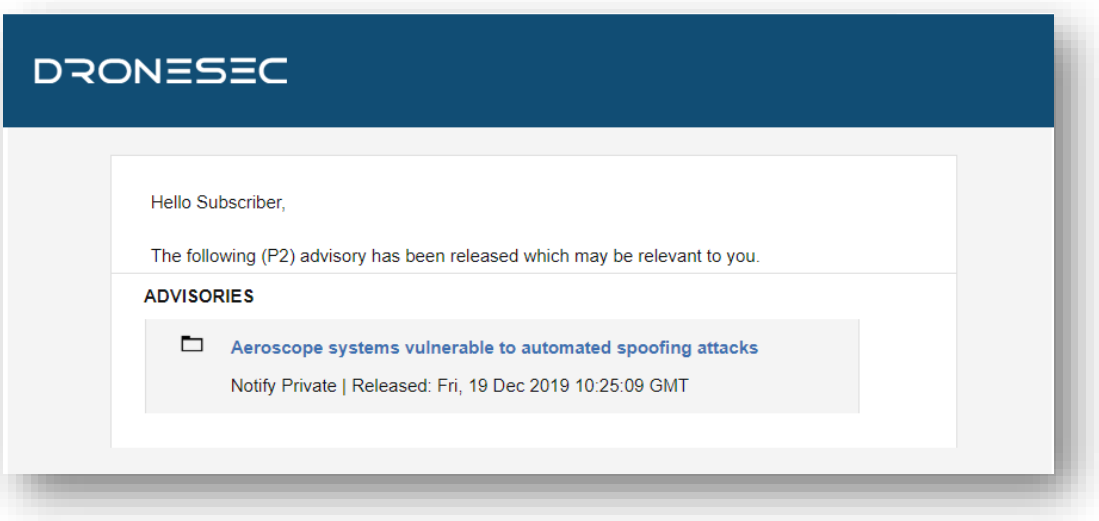


Figure 1 - A threat notification specific to a Notify customer's listed keywords.

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

Threat notifications are prioritised based on the following table:

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

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

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

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

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

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

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

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

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

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

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

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

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

APPENDIX B: SOURCES & LIMITATIONS

B.1. INTELLIGENCE SOURCES

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

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

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

B.2. LIMITATIONS

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

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

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