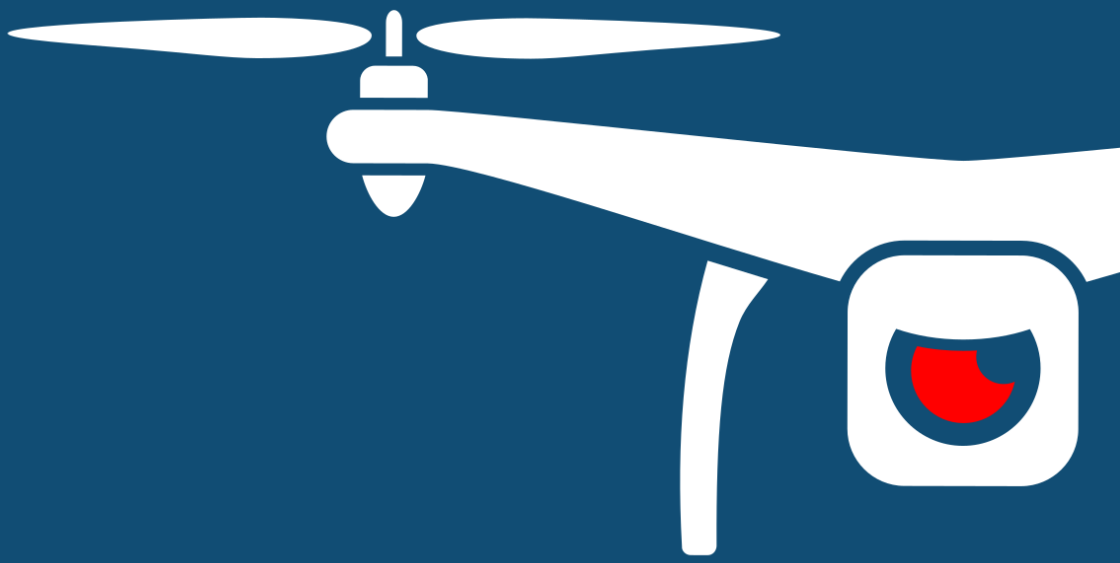
DRONE SEC
A Privasec COMPANY

NOTIFY ISSUE #60 (PUBLIC)

WEEKLY THREAT INTELLIGENCE

03 February 2021 | v1.0 RELEASE



UAS HACKING, HARDENING AND DEFENCE

UAS PENETRATION TESTING
COUNTER-UAS CONSULTING
FORENSICS & INCIDENT RESPONSE
AERIAL THREAT SIMULATIONS
DRONE SECURITY MANAGEMENT PROGRAMS

DOCUMENT **CONTROL**

PREPARATION

DroneSec (dronesec.com)

Threat Intelligence Team

Email: info@dronesec.com

Phone: 1800 996 001 | + 614 7854 3434 (Urgent)

EXECUTIVE SUMMARY

This week contains our monthly roll-up of observed incidents for the week of January – and 2021. Its interesting to note that January 2021 had the 3rd highest number of prioritised drone incidents for over a year (since January 2020). This may be due to Christmas period sales, or the relaxing COVID19 laws allowing more people to venture outside without curfews.

Israel had multiple drones downed this month near the borders of Gaza and Lebanon. There is chatter surrounding the idea that Hamas/Hezbollah has gained access to a counter-drone technology of their own relating to the increase in seizing IDF drones. The IDF have claimed no information is at risk due to the drones' seizure by militants.

In Canada, a close call with a drone flying beneath a MEDVAC plane at night on approach, and in Australia a DJI Inspire 2 has crashed into a high-rise building, injuring one person. Drones are being used in North Wales to surveil properties for subsequent thefts, with law enforcement officials issuing a warning to the public.

As always, if you have comments or feedback, want to join in the discussion in our slack discussion group, or find the system that captures this information please don't hesitate to contact us.

- *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.

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 year, Notify features an aggregated summary of drone incidents, types and affected sectors in 2021 and collated numerical data on drone incidents for the year. Extended analytics with full database-searchable functionality is only offered to our paid members via the DroneSec Notify Platform.

Below you will find some handy statistics to measure correlation, location and systems involved over data we have collected for January 2021. Anything we have missed? Anything you would like to see? Drop us a note at info@dronesec.com to get in touch with the team.

A new year, and a quite recap at 2020

To review 2020 once again, DroneSec recorded two thousand two hundred and ninety-four (2,294) artefacts in the past year which roughly equates to about six (6) drone security artefacts per day. COVID-19 helped boost perception of drone use by law enforcement agencies which led to the massive growth in other sectors. However, this also gave rise to small time actors using drones for nefarious deeds. The statistics below are for the month of January to December 2020, Notify release #4 – #55.

Month	Number of Artefacts	Global number of artefacts per day	Month-on-month increase
January	135	4.3	N/A
February	139	4.8	4 (2.88%)
March	179	5.8	40 (22.34%)
April	192	6.4	13 (6.77%)
May	200	6.5	8 (4.00%)
June	219	7.3	19 (8.68%)
July	224	7.2	5 (2.32%)
August	206	6.6	-18 (-8.74%)
September	168	5.6	-38 (-22.62%)
October	253	8.2	85 (33.60%)
November	177	5.9	-76 (-42.93%)
December	202	6.5	25 (12.38%)
Total (2020)	**2294**	**6.27**	N/A

For the year of 2021, DroneSec will continue with its monthly rollup to track incidents, events and these categories/tags allows readers to visualise them on a month-to-month basis. The statistics below are for the month of January 2021: Notify release #56 – #59.

Month	Number of Artefacts	Global number of artefacts per day	Month-on-month increase
January	209	6.74	N/A
Total (2021)	**209**	**6.74**	N/A

The month of January 2021 saw a surge in the number of artifacts relating to regulations and publications as the United States laid a solid stand on the rules for drones, driving responses from industries, manufacturers and other countries' aviation authorities. The United States Federal Aviation Authorities (FAA) have set the stage by implementing rules for night-time drone operations, flight over moving vehicles and populace, and on the highly debated Remote Identification. These rules will create precedence for other nations to follow, giving more leeway for organisation and hobbyist to dry their drones, resulting in growing utility of drones worldwide.

Category	Number of Artefacts (Jan 2021)	Compared to Number of Artefacts (Dec 2020)	Difference
Featured Incident Reports	10	15	-5
Cyber and Information Security	9	4	+5
News and Events	44	37	+7
Whitepapers and Publications	43	36	+7
Counter-Drone Systems	16	27	-9
UTM Systems	22	25	-3
Drone Technology	21	29	-8

Incident Summary

DroneSec records news and events that revolve around the use of drones, their innovation, counter measures and development. We classify drone incidents as events where drones were used as a medium in the conduct of illicit acts. Events where drones were used for the transportation of weapons, narcotics and/or contraband across borders or restricted areas are classified as drone incidents. Similarly, events where drones were sighted to have infringed airspace boundaries of manned aircrafts or areas with no-fly-zones such as hospitals or airports are also classified as drone incidents.

January 2021 had quite an amount of drone related incidents, further increasing the overall trend of drone incidents since the Year 2020. Having an increasing number of related incidents is not a good sign as this reflects the mindset of terror groups and small state actors on the advantages and use of drones to commit crimes.

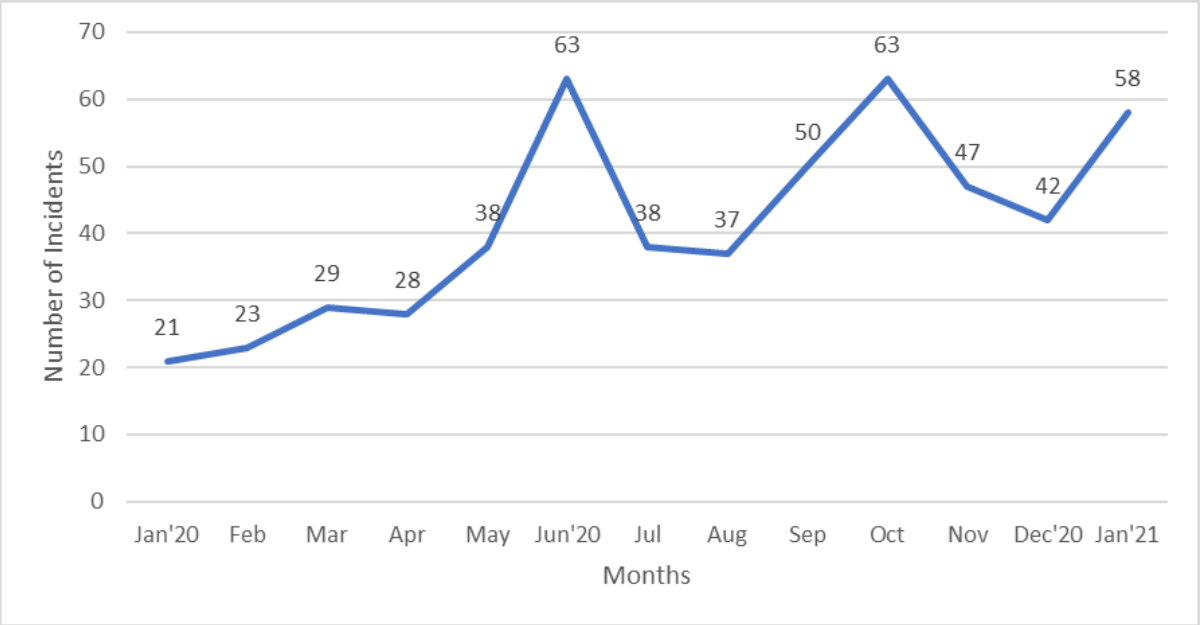


Figure 1: Number of Incidents Since January 2020

For restricted areas that have no-fly-zones (NFZs), DroneSec categorised these areas into eight different sectors. The month of January 2021 saw a large number of drone incursions across national borders in multiple countries, of note, India-Pakistan, and in open areas. Also, January 2021 recorded six drone deliveries into prisons, with two of the incidents where offenders flew their drone in on two occasions before getting caught.

While it is plausible to install drone detection and mitigation systems at these places, the cost of such systems outweighs the price of a drone and the replaceability of downed systems to nefarious operators. DroneSec recommends implementing drone security and risk management plans to handle such drone incidents into restricted areas.

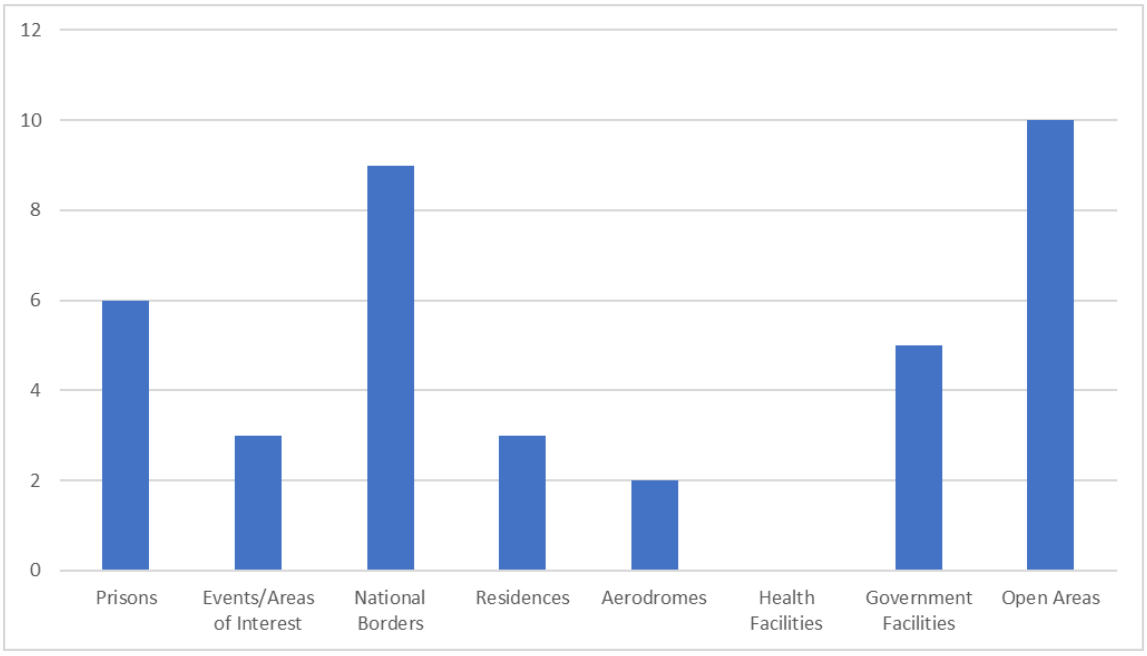


Figure 2: Number of Drone Incidents by Location of Occurrence (since January 2021)

DroneSec categorises all incidents recorded by country of occurrence. In 2021, the United States, India, Yemen and Syria logged almost 50% of all incidents faced globally. Incidents in the United States are mostly hobbyists / small time actors that resulted in crashes or intrusions into restricted areas.

For the remaining three countries, incidents were mainly due to terrorist groups using drones to fly across borders for deliveries of contraband or as a suicidal drone targeting residential or military areas.

The widespread use of drones in the United States and India have also led to strict drone laws implemented to ensure safe drone flights. However, for Yemen, Syria and even India, it is difficult to deal with terrorist organisations as laws are not enforceable and operators will continue to fly their drones irresponsibly to achieve their intended aim.

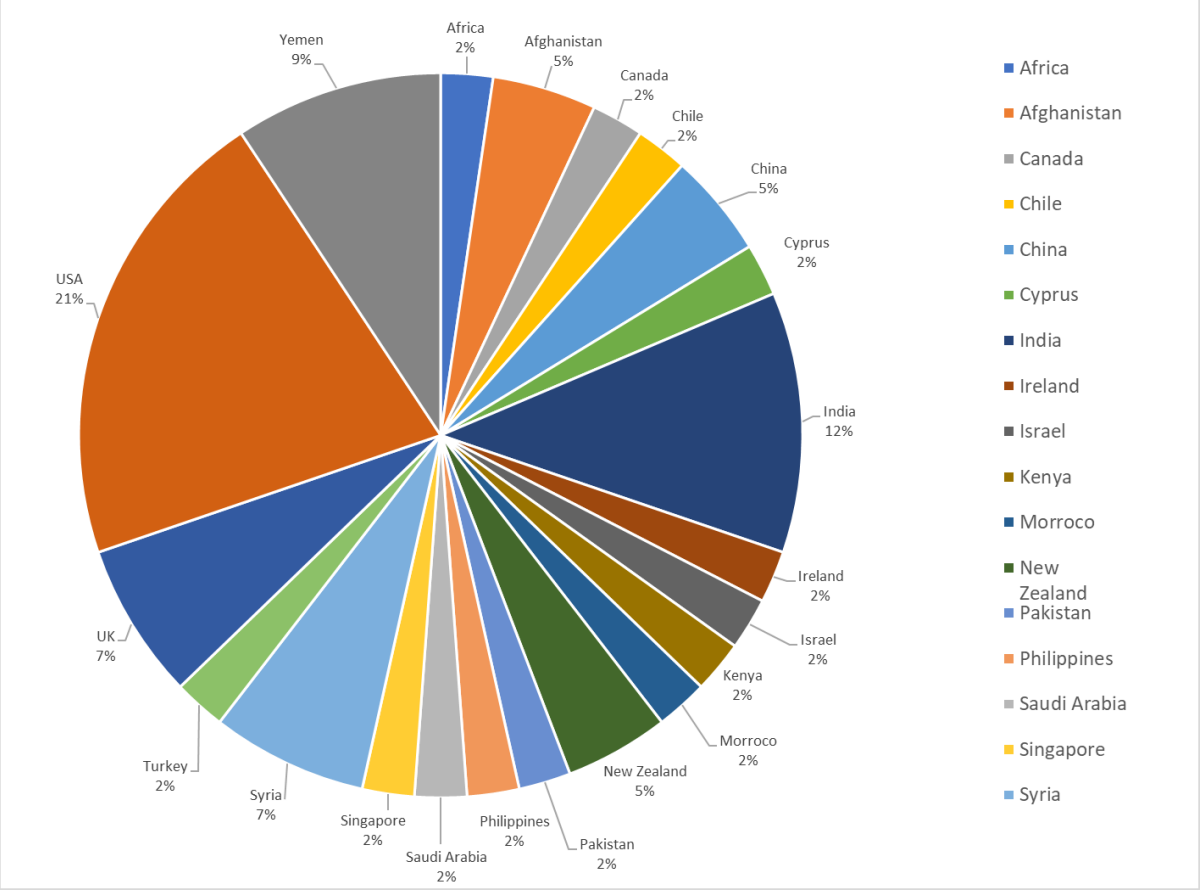


Figure 3: Percentage of Drone Incidents by Country of Occurrence (Since January 2021)

For all the drone incidents that were recorded in January 2021, DroneSec observed seizure of drones by law enforcement agencies in 64% of incidents. This is a relatively higher figure than 2020 (57%), but the eventual number may gear towards that throughout the remaining months of 2021. Of the remaining 36% cases, the drones were not found despite a thorough search in the vicinity. Some key installations are well equipped with Standard Operating Procedures (SOP) on handling drone incursions and were able seize the opportunity when a drone was spotted, whereas others were not successful in their attempts despite engaging external security practitioners.

Of note, most areas which have reported success in seizing drones were areas that have faced multiple drone intrusions before. However, DroneSec is starting to see more restricted areas facing drone incursions and security personnel who are not prepared for such incidents, leading to the drone accomplishing its task and escaping before any mitigation action can be performed.

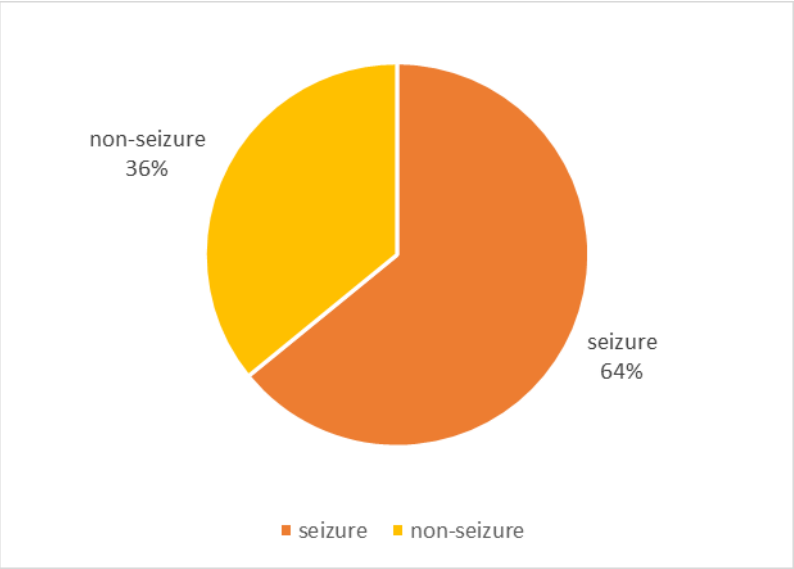


Figure 4: Percentage of Drone Incidents Where the Drone was Seized (Since January 2021)

Conversely, only 31% of rogue drone operators were apprehended for their illicit act(s) in January 2021. Not only are drones small and versatile in escaping from the detection of law enforcement agencies, but it also creates a distance between the operator and the area of operations. Nefarious operators will use this to their advantage and flout drone laws to conduct their illegal activities as risk of apprehension is reduced. Law enforcement agencies who have seized drones should also request for digital forensic analysis on the data stored within the drones. Important information such as flight details, time of journey, take off locations and images and video footage of the environment and operator's face may be evident within. This information will help to bridge the gap in tracing and arresting the offender.

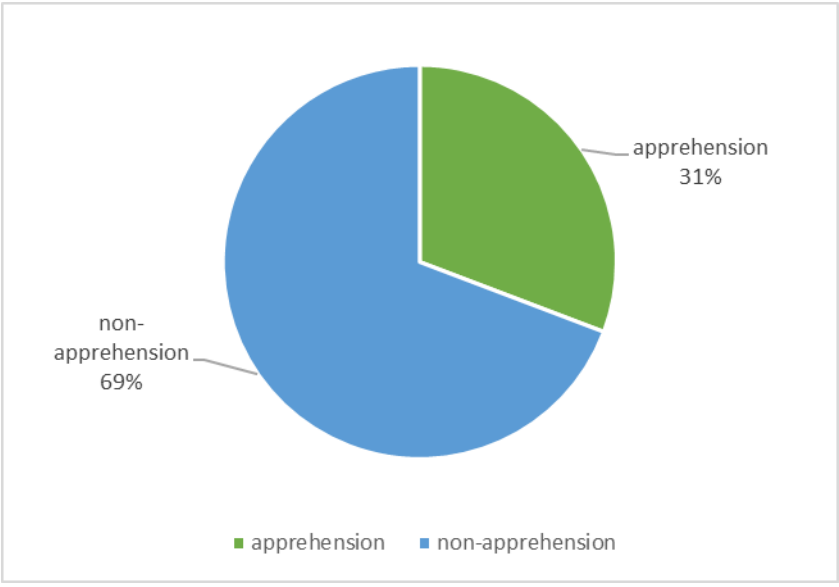


Figure 5: Percentage of Drone Incidents Where the Drone Operator was Apprehended (Since January 2021)

The difference in percentage on the seizures of drones against the apprehension of the drone operators shows that counter drone systems may only be geared towards the detection and capture of rogue drones. The gap in arresting the operator responsible continues to exist, which should be addressed, otherwise, malicious use of drones will only continue to increase over time.

DroneSec believe that the implementation of Remote Identification and UAS Traffic Management (UTM) systems in the near future will see more errant drone operators tracked and discovered. For now, eyewitnesses or manual tracking (following the drone) to its operator will be the interim solution, or otherwise, using data extraction forensic tools on downed drones to retrieve video footages, telemetry and flight logs.

That concludes our monthly roll up for the artefacts we have consolidated for January 2021.

1.3. FEATURED ADVISORIES

The prioritisation table and its dependencies are explained in Appendix A, and relate to how we filter, analyse and visualise the intelligence we collect.

Figure 6 - Can't see this incident report? Email info@dronesec.com to access our private reports.

1.4. NEWS AND EVENTS (P2)

Russian quadcopter allegedly dropped VOG-17 grenade on two Ukrainian troops

https://menafn.com/1101515484/Two-Ukrainian-servicemen-wounded-in-drone-strike-near-Vodiane

Alleged counter drone technology used by Hamas terror group to crash IDF drone

https://www.jpost.com/breaking-news/idf-drone-crashes-in-gaza-strip-report-657356

Israeli drone shot down and seized by Hezbollah performing recon near Lebonese border

https://federalnewsnetwork.com/government-news/2021/02/lebanons-hezbollah-group-says-it-shot-down-israeli-drone/

Israel loses quadcopter at Gaza Strip, drone seized by Hamas terrorist group

https://www.jpost.com/israel-news/for-third-day-in-a-row-idf-quadcopter-falls-outside-israels-borders-657503

Arab Coalition destroys armed Houthi drone flying in Saudi Arabia

https://www.arabnews.com/node/1801011/saudi-arabia

North Wales PD issues warning as drones are used to stake out farms to plot robberies

http://www.deeside.com/warning-issued-as-thieves-use-drones-to-stake-out-farms-in-north-wales/

DJI Inspire 2 drone loses control and crashes into high-rise building at high speed, injuring one

https://www.atsb.gov.au/publications/investigation_reports/2021/aair/ao-2021-001/ (Official Source)

https://australianaviation.com.au/2021/01/drone-crashes-through-darling-harbour-window-injuring-occupant/

Drone spotted conducting night-time operations nearby Ravenhall Prison, Australia

(Community report)

1.5. SOCIALS (P3)

USAF MQ-1C drone makes emergency landing in Niger with locals reaching the system first

https://www.instagram.com/p/CKjZisKpSXE/

Canadian man charged for using drone during hunting trip

https://www.facebook.com/ConservationOfficerService/posts/5104809722893871

1.6. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P3)

India imposes ban for drone flights in Bengaluru due to Aero India air show

https://www.ndtv.com/bangalore-news/aero-india-event-drones-quadcopters-banned-from-flying-in-bengaluru-due-to-aero-india-2360600

Israel drafts new regulations to allow use of 5.8GHz frequency for civilian drones

https://www.unmannedairspace.info/latest-news-and-information/new-draft-drone-rules-will-open-up-drone-market-in-israel-for-more-complex-operations/

Drone Swarms Are Getting Too Fast For Humans To Fight (commentary)

https://www.forbes.com/sites/davidhambling/2021/01/27/drone-swarms-are-getting-too-fast-for-humans-too-fight-us-general-warns/?sh=398b4807372c

Singapore public less keen on drone use in residential zones than industrial zones (commentary)

https://techxplore.com/news/2021-01-singapore-keen-drone-residential-areas.html

Growing drone uses raise new international law challenges (commentary)

https://www.engineeringnews.co.za/article/growing-drone-uses-raise-new-international-law-challenges-2021-01-29/

Drones: New normal in hybrid warfare (commentary)

https://www.dailyexcelsior.com/drones-new-normal-in-hybrid-warfare-2/

Al-Qaeda, CPEC, Drone Warfare: Your briefing from Afghanistan and Pakistan (commentary)

https://gandhara.rferl.org/a/al-qaeda-cpec-drone-warfare-afghanistan-pakistan-briefing/31076499.html

Drones over Riyadh: Unpacking the Iran Threat Network's Tactics (commentary)

https://www.washingtoninstitute.org/policy-analysis/drones-over-riyadh-unpacking-iran-threat-networks-tactics

Twenty seconds to foil an attack: The secrets of the Italian army's anti-drone squad (commentary)

https://www.corriere.it/speciale/cronache/2021/squadra-antidrone/

Taliban PsyOps: Afghan Militants Weaponise Commercial Drones (commentary)

https://gandhara.rferl.org/a/taliban-commercial-drones-attacks-afghanistan/31075672.html

FAA could strengthen its implementation of a drone traffic management system by improving communication and measuring performance (USA Government Accountability Office)

https://www.gao.gov/assets/720/712037.pdf (PDF Document)

1.7. CYBER AND DATA SECURITY (P4)

Users looking to buy attacks/hacking exploits for Ocusync, Ocusync 2.0 protocols

Community submission

Angoka partners Connected Places Catapult to better secure drone communication channels

https://businessmk.co.uk/drone-security-experts-join-forces-to-thwart-hijack-threat-and-boost-commercial-potential/

Intelligent Network Layer for Cyber-Physical Systems Security

https://arxiv.org/pdf/2102.00647.pdf (PDF Document)

1.8. COUNTER-DRONE SYSTEMS (P4)

Citadel Defense receives multi-million dollar contract for Titan AI CUAS system

https://www.geospatialworld.net/news/citadel-defense-wins-govt-contract-for-ai-powered-counter-drone-system/

Boeing unveils Bofors 3P counter drone ammunition

https://militaryleak.com/2020/12/09/bae-systems-bofors-3p-counter-uas-ammunition/

North Korea reportedly pushing for mass production of drones for surveilling border

https://www.dailynk.com/english/north-korea-moves-toward-mass-production-miniature-reconnaissance-drones/

OpenWorks SkyWall Patrol tested and evaluated for EU law enforcement project, SKYFALL

https://openworksengineering.com/more-european-police-choose-skywall-net-capture-following-competitive-tender/

Northrop Grumman and Pierce Aerospace collaborate to expand Remote ID capabilities in CUAS and UTM systems

https://www.unmannedairspace.info/latest-news-and-information/northrop-grumman-pierce-collaboration-aims-to-expand-market-reach-for-small-business-remote-id-services/

Dedrone offers Remote ID capabilities to USA and EU via DroneDNA

https://www.dedrone.com/press/dedrone-first-to-offer-both-united-states-and-european-union-drone-remote-id-capability

RF Enables Takeover of Hostile Drones (commentary)

https://www.darkreading.com/iot/rf-enables-takeover-of-hostile-drones/a/d-id/1339944

Pentagon to field low-collateral, counter-drone interceptors in FY22 (commentary)

https://www.defensenews.com/land/2021/02/02/pentagon-shoots-to-field-low-collateral-counter-drone-interceptors-in-fy22/

1.9. INFORMATIONAL (P5)

Fire Rescue Victoria sets up drone unit to better monitor fires and emergencies

https://www.itnews.com.au/news/fire-rescue-victoria-sets-up-new-drone-unit-560393

Alexander County PD uses drone with thermal imaging to find missing 78-year-old man

https://www.wcnc.com/article/life/people/deputies-use-thermal-imaging-drone-to-rescue-78-year-old-man-from-embankment/275-91e88537-8088-457b-bdbd-9e3d56c8b9b1

Rutherford County PD locates teenager in freezing water with help of thermal imaging drone

https://www.dnj.com/story/news/local/2021/01/31/missing-juvenile-rutherford-county-located-drone/4332535001/

Malaysia Armed Forces use drones to ensure Sibu residents comply with COVID-19 lockdown

https://www.malaymail.com/news/malaysia/2021/02/02/armed-forces-use-drones-to-encourage-sibu-residents-to-comply-with-sop/1946350

F-35s and Drones Can and Will Be Networked Together (commentary)

https://nationalinterest.org/blog/buzz/f-35s-and-drones-can-and-will-be-networked-together-177196

1.10. UTM SYSTEMS (P5)

Vertical Aerospace receives £2.5M grant to test feasibility of air taxis in United Kingdom

https://www.internationalairportreview.com/news/151035/uk-feasibility-project-electric-air-taxis-government-grant/

Urban Air Port Air-One secures funding from UK government

https://www.hyundai.news/eu/brand/world-first-electric-urban-air-portr-secures-uk-government-backing/

H3 Dynamics and Thales trials real-time autonomous drone flight monitoring system

https://www.suasnews.com/2021/01/thales-and-h3-dynamics-enter-drone-automation-age-with-real-time-tracking-for-seamless-traffic-control-in-low-altitude-airspace/

Kongsberg Geospatial, uAvionix and Aireon to demonstrate space-based airspace picture for BVLOS drone operations

https://www.einnews.com/pr_news/535093505/kongsberg-geospatial-improves-bvlos-drone-operations-safety-with-a-horizonless-air-picture

SK Telecom joins partnership to develop UAM in South Korea

https://www.sktelecom.com/en/press/press_detail.do?page.page=1&idx=1496

Airmap suggests drone airspace should be monetized, sparking outrage (commentary)

https://petapixel.com/2021/01/28/airmap-suggests-drone-airspace-should-be-monetized-sparking-outrage/

1.11. DRONE TECHNOLOGY (P5)

IAI secures more than USD100M worth of sales on suicide drones, Harop and Rotem

https://www.iai.co.il/iai-to-provide-loitering-munitions-to-asian-countries-deals-worth-over-100-million-usd

UK trials swarm of 20 drones utilising Blue Bear's mobile command and control system

https://www.airforce-technology.com/news/uk-flies-20-drone-swarm-in-major-test/

Holo demonstrates detect and abort capability from medical helicopter at Denmark's U-Space

https://www.unmannedairspace.info/latest-news-and-information/danish-u-space-demonstration-in-odense-plans-vlos-flights-in-shared-airspace/

USA Marine Corps contracts Metal Shark to develop suicide drones on unmanned vessels

https://www.washingtontimes.com/news/2021/jan/27/marine-corps-moves-ahead-kamikaze-drone-project/

HAL to display fighter-drone teaming prototype at Aero India 2021

https://www.defenseworld.net/news/28878/India_s_HAL_to_Display_Teaming_Drone_at_Aero_India_2021

Zenith AeroTech reveals tethered drone Quad 8, with flight radar and mobile networked radio

https://zenithaerotech.com/zenith-aerotech-mounts-radar-networking-radio-and-eo-ir-camera-on-small-tethered-drone-integration-demonstrates-versatility-of-long-endurance-heavy-lift-readily-deployable-quad-8/

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.

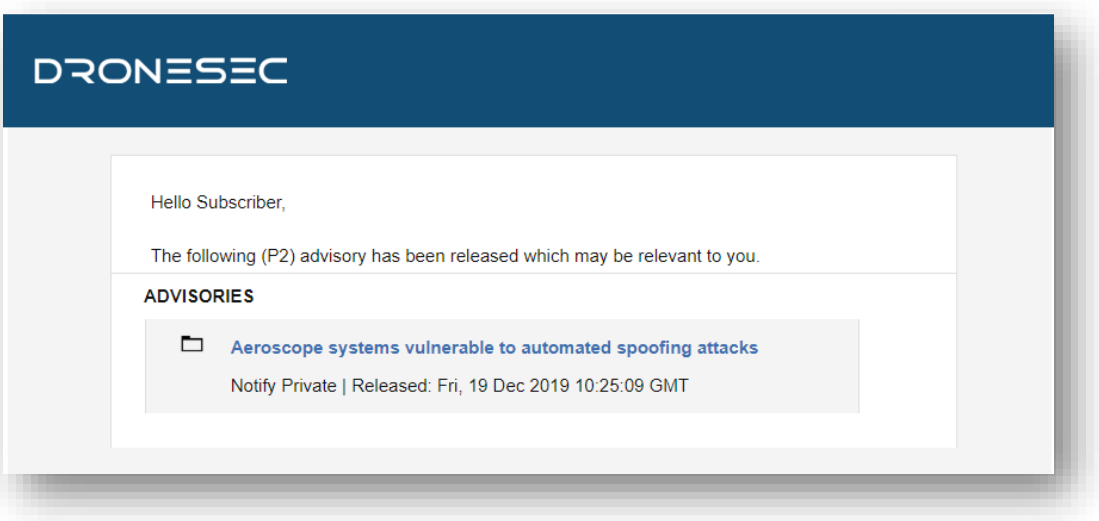


Figure 7 - A threat notification specific to a Notify customer's listed keywords.

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.