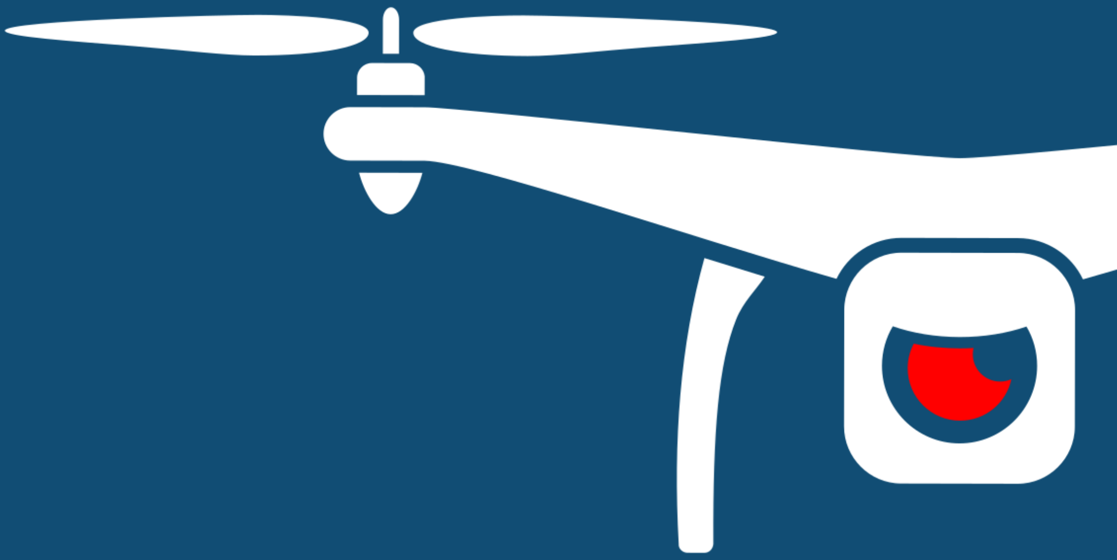
DRONE SEC

A Privasec COMPANY

# NOTIFY ISSUE #14

## WEEKLY THREAT INTELLIGENCE

19 March 2020 | v1.0 RELEASE



UAS HACKING, HARDENING AND DEFENCE

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

# DOCUMENT **CONTROL**

## PREPARATION

DroneSec (dronesec.com)

Threat Intelligence Team

Email: info@dronesec.com

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

# EXECUTIVE SUMMARY

As COVID-19 extends to other countries around the world, we are seeing the initial innovation in drones as a response solution in China now occurring in Western countries. Some hiccups with regulatory issues restricting some of these initiatives are still happening, but progress nevertheless (and a motivational jab to UTM/UAM efforts). The team here at DroneSec is hoping you are all safe and well – we're working remotely at the moment and are prioritising outback drone flights away far from the city stockpiling.

This week there is a fair bit of informational material that might not fit immediately into a 'security' agenda for drones. We've had multiple requests for this information to be included as it provides key information to security outfits in preparing for or responding to an incident. Given incidents are based on a specific drone type, it helps to prepare by knowing how many and for what use they are being used in the industry. For this reason, catering to a myriad of different drone types is an important metric and one we hope to provide a birds-eye view on.

This week the Defense Innovation Unit (DIU) has placed a call for commercial solutions to help the United States Department of Defense improve small drones by using better flight controllers, sensors and datalinks. *Submissions should include what drones their solution has been installed on. Successful prototypes will demonstrate interoperability, be able to integrate into DoD small unmanned systems and comply with Section 848 of the National Defense Authorization Act for Fiscal Year 2020.* It's been interesting seeing the commentary around this - especially where some DoD personnel have grown up accustomed to XBOX gaming controllers and the like; making current drone control systems in a similar manner may speed up operator onboarding and provide a familiar sense of control.

I'll be sending out a personal letter to some of our subscribers this week to inform them of our upcoming BETA test for the DroneSec Notify Threat Intelligence Platform (TIP). We are around the corner from launch and have a limited number of opportunities available for discounted subscriptions before the full pricing suite comes into effect late April. All things considering, we're looking for firms willing to help provide feedback with novel and unique environments that will aid in our testing process. You can get in touch with me personally to discuss this opportunity.

- *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](mailto:info@dronesec.com). Otherwise, feel free to hop into the slack channel and introduce yourself: [DroneSec Slack Channel](). If you missed the previous issue, please email us.

# 1.2. FEATURED ADVISORIES (P2)

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

| Security | Tags | Priority |
|---|---|---|
| Multiple drone smuggling activities conducted against Fort Dix federal prison, New Jersey | Drones, Critical Infrastructure & Security | P2 |

**Summary**

At least seven drone deliveries were made into a low security prison in New Jersey before the offenders were caught after an inmate was found possessing contraband items. Drones were used to conduct the deliveries.

**Overview**

Marijuana, steroids, syringes, saw blades, cell phones and SIM cards were found packed in a parcel that was initially tied to and dropped by a drone. The duo had made seven deliveries since July 2018 and were arrested when fingerprints recovered from the package matched theirs. The initial discovery was found when an inmate was first apprehended near the parcel drop site with 34 cell phones, 9 chargers and 51 SIM cards. The two men were arrested shortly afterwards just outside the prison with the drone in their vehicle.

**Analysis**

In most cases, drone incidents are caused by a repeating offender or organised group. The low price point and availability of COTS drones means an easily accessible tool to conduct illegal acts with not too much risk of being apprehended (drones are disconnected from the controller by distance and wireless transmissions). Furthermore, the skill barrier to be able to fly a drone is not complex, and incidents often see offenders becoming lax with their approach and utilising the same take-off/landing points as before.

There is little identification of confirmed cases in which rogue operators are utilising 3/4G mobile technologies, autonomous GPS routes or one-way drone flights; to this point in time apprehending operators is made easier by currently available drone detection and alert systems.

**Recommendation**

All prisons should have a Drone Security Management Plan in place to deal with small unmanned systems, whether or not Counter-Drone systems are in place within the environment. A standard operating procedure (SOP) should govern the process, people and methodology in handling a drone, collecting evidence and responding to potential operators in a pre-determined radius around the prison grounds.

Any incident should be logged, categorised and reported to local law enforcement. Event analysis should take place by determining if the drone was similar to previous cases, took similar launch/land flight paths and as much footage of the device captured as possible. This information can aid correctional facilities in practicing and timing their response, undergoing challenges faced in communication and regulatory requirements, and providing investors or stakeholders with assurance as to risk planning.

Finally, correctional facilities that are in Counter-Drone-denied environments (whether regulatory or financially) should seek detection systems that do not seek to necessarily mitigate but do provide tracking and post-incident analysis capabilities.

**References**

- https://edition.cnn.com/2020/03/15/us/new-jersey-prison-drone/index.html

| Safety and Security | Tags | Priority |
|---|---|---|
| Close-proximity incident between military helicopter and drone | Drones, Safety, Commercial, Military | P2 |

**Summary**

During an army exercise, a drone captured video footage of a military helicopter flying into its path and taking evasive action to avoid collision.

**Overview**

A Mi-24 military attack helicopter had to take evasive action after spotting a drone in its flight path during a military exercise in Russia. A video uploaded with the perspective from the drone's camera, was posted on social media showing the near air proximity between the drone and the helicopter. No further details were provided by the Russian military after the incident.

**Analysis**

A study from the FAA concluded that drone strikes caused more damage to aircrafts and helicopters than bird strikes, making drones a real threat to the safety of civil and military aviation. Due to the rigid components of drones, these materials when ingested flew much deeper into the engine and dealt a greater proportion of damage compared to animals. Nowadays, capabilities of drones have progressed to being able to fly further and higher, some even allowing operators to fly the drone beyond visual line of sight (BVLOS). These advancements are beneficial when utilised correctly, for example in search and rescue operations, but cause harm when not adhering to regulations set in place by authorities.

**References**

- https://defence-blog.com/army/mi-24-helicopter-came-close-to-drone-collision-during-a-military-exercise.html

| Safety | Tags | Priority |
|---|---|---|
| DJI Matrice 210 loses battery power falling into the Atlantic Ocean | Drones, Safety, Military | P2 |

**Summary**

During a joint training exercise, a drone was ditched into the sea due to low battery power and strong head winds which prevented the drone from arriving at its landing point.

**Overview**

A $26,000 DJI Matrice 210 used in a joint training exercise for surveillance during rescue operations crashed into the ocean prior to recovery due to strong headwinds and low battery power. Instead of landing the drone onto one of the participating boats, the operators decided to conduct a controlled crash of the drone into the ocean as there could be safety implications for personnel onboard if an attempted landing was made. Due to this incident, authorities will be adjusting their protocols to such conditions over water to ensure drones are sent 'home' much earlier.

**Recommendation**

It's recommended that drone operators have a good understanding on the capabilities of their drones – flight time, range and protocols or frequencies in use. These are important details which aid operators in planning their pre-flight mission and handling ad-hoc changes when unexpected contingencies may occur mid-flight.

**References**

- https://dronedj.com/2020/03/13/26000-dji-matrice-210-lost-to-the-ocean-during-training-exercise/

| Safety and Security | Tags | Priority |
|---|---|---|
| Quadcopter with carrying explosive payload crashes wounding six servicemen | Drones, Safety, Military, | P2 |

**Summary**

A military drone (quadcopter) lost control during a training session and crashed, detonating the onboard explosives and wounding six nearby servicemen.

**Overview**

During a training drill in Russia, Marine Brigade No. 61 was practising drone combat operations when the quadcopter lost control and crashed into the ground. As the drone was carrying simulated explosives, the crash dispersed shrapnel on impact wounding the nearby servicemen.

Sources suggest it was a small quadcopter drone, being utilised for training separate to the larger, more commonly known military UAV systems. The incident was said to have violated safety requirements with no further details from the military unit.

The cause of the disruption to control systems is unknown – no confirmation has been made on operator mistake or interdiction to transmission or communication functions.

**References**

- https://www.mirror.co.uk/news/world-news/out-control-military-drone-wounds-21635246

## 1.3. NEWS AND EVENTS (P3)

**100 drones with inter-state intelligence sharing to monitor religious event in India**

https://www.newindianexpress.com/nation/2020/mar/16/uttarakhand-100-drones-1500-cctvs-to-monitor-mahakumbh-crowd-2117176.html

**Owensboro Police create UAS unit to utilise DJI Mavic for SAR, SWAT and LE activities**

https://www.owensborotimes.com/news/2020/02/opd-implements-unmanned-aerial-vehicle-team/

**Northamptonshire Police carry drones in patrol cars**

https://www.daventryexpress.co.uk/news/crime/cutting-edge-policing-technology-more-northamptonshire-police-officers-trained-use-drones-2455608

**Moulton Police Department infrared camera drone aides in three chase arrests**

https://www.moultonadvertiser.com/news/local/article_b92541b0-63cb-11ea-9ab4-53bb29974730.html

## 1.4. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P3)

**India sets 6 green zones of 5km radius for unhindered drone flying**

https://www.indiapost.com/indias-first-6-green-zones-for-drone-ops-get-security-clearance/

**European Aviation Safety Agency (EASA) framework on mitigating air and ground risks**

https://www.easa.europa.eu/document-library/opinions/opinion-012020#group-easa-downloads

https://www.easa.europa.eu/sites/default/files/dfu/Draft%20COMMISSION%20IMPLEMENTING%20REGULATION%20on%20a%20high-level%20regulatory%20fram....pdf

**Safety feasibility of last-mile drone delivery from a regulatory perspective (Commentary)**

https://finance.yahoo.com/news/feasible-drones-last-mile-delivery-145523767.html

**Australian CASA launches National Drone Safety Campaign targeted at drone hobbyists**

https://www.casa.gov.au/knowyourdrone

**DJI files 89-page formal comment urging FAA to reconsider their Remote ID rule for drones**

https://www.dji.com/newsroom/news/dji-urges-faa-to-reconsider-flawed-remote-id-rule

## 1.5. COUNTER-DRONE SYSTEMS (P4)

**Harp Arge develops Turkey's first lightweight (2.5kg) anti-drone EM interference gun**

https://www.dailysabah.com/business/defense/local-manufacturer-unveils-lightweight-anti-drone-gun

**Raytheon approved for sale of Coyote Block 2 counter-drone weapon – detection and missile**

http://investor.raytheon.com/news-releases/news-release-details/coyote-block-2-counter-drone-weapon-approved-international-sales

**Joint Counter Small Unmanned Aerial Systems (C-sUAS) Office on final C-UAS selection**

https://breakingdefense.com/2020/03/dod-winnowing-efforts-to-counter-small-drones/

**VigilAir RF-based drone detector gets UK certification on protection of critical infrastructure**

https://www.suasnews.com/2020/03/vorpals-vigilair-counter-drone-technology-gets-uk-cpni-certification/

## 1.6. UTM SYSTEMS (P4)

**AirMap's UTM partners with Skyguide for digital authorisation of drone flights in Switzerland**

https://www.airmap.com/skyguide-unveils-digital-and-automated-authorization-system-for-uas-and-special-flights-in-controlled-airspace-switzerland/

**Frequentis and HENSOLDT to combine for integrated UTM/Drone detection, data fusion and air traffic monitoring system**

https://www.aviationpros.com/airports/airport-technology/press-release/21129435/frequentis-usa-inc-integrated-counter-uav-solution-led-by-frequentis-and-hensoldt

**AirMap lays groundworks to develop drone traffic control system**

https://www.digitaltrends.com/cool-tech/airmap-air-traffic-control-for-drones/

## 1.7. DRONE TECHNOLOGY (P5)

**HAPSMobile mobile drone-based broadband to commence trials in Queensland in 2021**

https://www.itnews.com.au/news/hapsmobile-to-run-drone-broadband-trial-in-queensland-skies-539196

**New Zealand invests $790k in drones conducting predator-control activities**

https://www.beehive.govt.nz/release/new-predator-control-drones-help-nature-hard-reach-place?utm_source=miragenews&utm_medium=miragenews&utm_campaign=news

**South Dakota State University develop human-transport drones under NASA grant**

https://www.keloland.com/news/eye-on-keloland/sdsu-students-working-on-drone-capable-of-carrying-a-person/

**Spanish police use drones with loudspeakers to demand people return home**

https://www.forbes.com/sites/zakdoffman/2020/03/16/coronavirus-spy-drones-hit-europe-police-surveillance-enforces-new-covid-19-lockdowns/#3c35fb517471

**Adelaide's confirm 2020 New Year's Eve to utilise drone light show over fireworks**

https://www.abc.net.au/news/2020-03-11/drones-and-lasers-incorporated--into-adelaide-nye-fireworks/12044932

**DJI Inspire 1 & DJI Matrice 210 used for HAZMAT response by Southern Manatee Fire Rescue**

http://www.uavexpertnews.com/2020/03/dji-drones-can-be-used-for-hazmat-response/

**Matternet's drone logistic solution to be deployed in US and Switzerland hospital systems**

https://venturebeat.com/2020/03/10/matternets-station-is-a-safe-drone-portal-for-hospitals/

## 1.8. INFORMATIONAL (P5)

**Turkey establishing combat drone base for counter-terrorism measures**

https://www.dailysabah.com/business/defense/turkey-to-build-drone-base-in-eastern-erzurum-province

**Spanish Department of Traffic supplied with 28 drones for surveillance and regulation**

https://www.aviationpros.com/aircraft/unmanned/press-release/21129615/sdle-to-supply-drones-for-road-traffic-safety-in-spain

**India commences medical delivery platform by drones at Begumpet Airport**

https://www.newindianexpress.com/states/telangana/2020/mar/15/yes-drones-can-deliver-med-supplies-too-2116938.html

**Drone-carrying submarine motherships as a form of naval power (Commentary)**

https://nationalinterest.org/blog/buzz/submarine-motherships-navy-wants-drone-carrying-subs-wage-war-131602

**Isle of Wight to have drones deliver medical care from the UK mainland**

https://onthewight.com/isle-of-wight-chosen-for-government-pilot-to-test-drone-deliveries-of-medical-samples-across-the-solent-says-mp/

**Drones at Mexico border flown by people/drug smugglers swarming border (commentary)**

https://www.washingtonexaminer.com/news/government-fails-to-respond-as-drones-flown-by-people-smugglers-and-drug-runners-swarm-border-watching-agents

**Clarkstown Police utilise Drone Unit to rescue hiker stuck on cliff**

https://patch.com/new-york/newcity/cliff-rescue-stranded-hiker-haverstraw

# 1.9. SOCIAL (P5)

**Use of thermal imaging drones to detect buried or hidden explosive landmines**

“Made it back to Australia from Chad before borders started closing due to COVID-19. Just finished perhaps the most ambitious humanitarian landmine thermal imaging campaign from drones ever completed.

We set up an entire test site with dozens of real #landmines, containing real explosives (minus fuses) near our camp - inside a 25km perimeter of active 30-year-old legacy minefields. Systematic data capture of real landmines buried at a test site - plus flying data from active minefields - captured at the same time.

The expedition took place with Handicap International - Humanity & Inclusion Handicap International Belgium under the auspices of the High Commission for Demining in Chad (the HCND) and was funded by the Belgian Ministry of Foreign Affairs.

Special thanks are in order to; Abdourahmane Ba who worked 19 hours a day, Jason Mudingay who came to wadidoum - even while ill, and Kheira Djouhri who battled logistical hurdles every step of the way.

https://www.linkedin.com/posts/john-fardoulis-91a3783a_australia-chad-humanitarian-activity-6646003189126692864-cBDJ

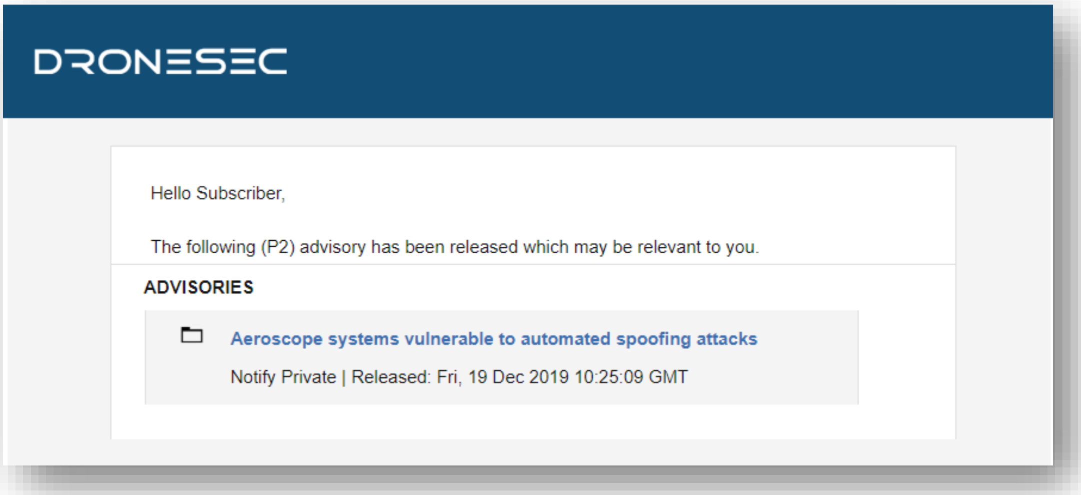
# APPENDIX A: THREAT NOTIFICATION MATRIX

## A.1. OBJECTIVES

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

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

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



DRONESEC

Hello Subscriber,

The following (P2) advisory has been released which may be relevant to you.

ADVISORIES

Aeroscope systems vulnerable to automated spoofing attacks

Notify Private | Released: Fri, 19 Dec 2019 10:25:09 GMT

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

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

Threat notifications are prioritised based on the following table:

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

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

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

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

| Tag - Categories | Description |
|---|---|
| Drones | Custom-made or Commercial-Off-The-Shelf (COTS) systems that might:<br>• Be known as UAS[1], UAV[2], RPAS[3]…<br>• Weigh 50g all the way to 250kgs<br>• Are automated or manually piloted<br>• Have associated devices, software or infrastructure |
| CUAS | Counter-UAS systems that might:<br>• 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<br>• Be standalone, hand-held, static or integrated with a UTM[4] or PSIM[5] system<br>• Have associated systems, software, infrastructure and communication protocols |
| UTM | Universal Traffic Management system that might:<br>• Be known as Urban Air Mobility (UAM) or fleet management systems<br>• Manage, track, communicate with or interdict drones and/or drone swarms<br>• Be software and/or hardware based<br>• 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<br>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<br>Studies and Reports |
| Pilots – Commercial and Private Airlines | Pilots currently active in the commercial or private airline industry. | AirProx Reports<br>Visual Identification Reports |
| Commercial Partnerships | Our partners in the military defence, commercial vendor and security industry exchange intelligence with Notify. | Statistics<br>Incidents<br>Sentiment and chatter<br>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<br>Whitepapers<br>Research Papers<br>Vulnerabilities and Exploits<br>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<br>Incidents |

| | | |
|---|---|---|
| | Security, threat intelligence and Open-Source Intelligence (OSINT) communities provide Notify with recent, actionable information. | Whitepapers<br>Research Papers<br>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<br>Incidents<br>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<br>Incidents<br>Statistics |
| Proprietary aggregation software<br>- Search Engines<br>- Social Media<br>- 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<br>Events<br>Incidents<br>Whitepapers<br>Research Papers<br>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<br>Research Papers<br>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.