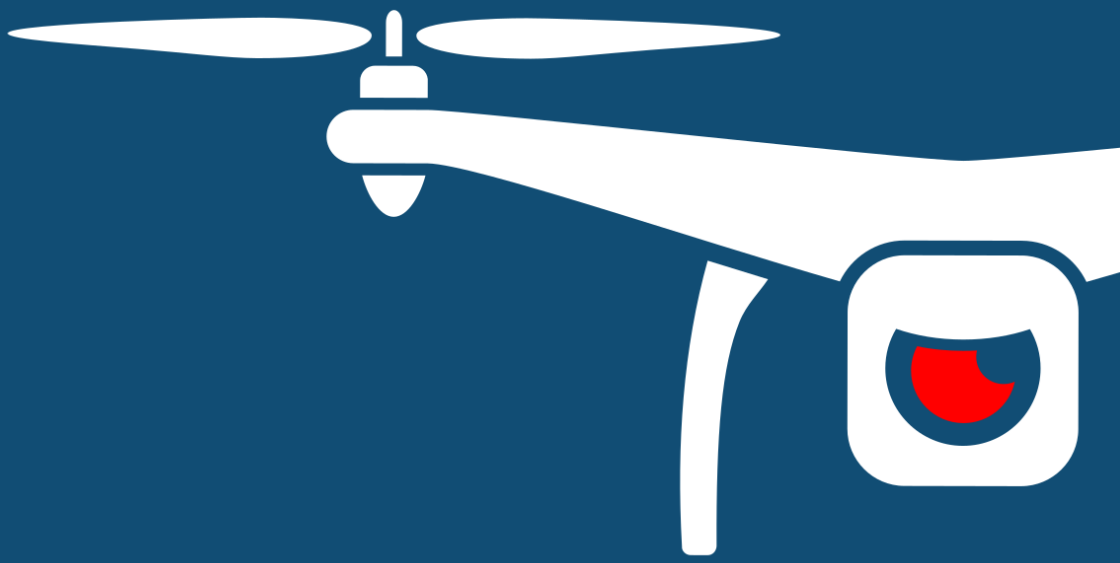
DRONE SEC
A Privasec COMPANY

NOTIFY ISSUE #44 (PUBLIC)

WEEKLY THREAT INTELLIGENCE

14 October 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

Some key information for both readers and platform users – from next week, Threat Actor Profiles will be living resources as part of our Threat Actor Glossary. This means that they will be referenced within reports like these but displayed within a live webpage. The reason for this is the ever-evolving tactics, techniques and procedures used by different threat actors. We need to reflect the full story as developments occur and update these on the fly once attribution has been triaged. These profiles will be publicly available and we encourage contributions.

This week we see a first narco-drone incident occur in one of Spain's autonomous cities located in North Africa. Also, a court case for drone intrusions at Fort Dix prison reveal how aerial photographs with markings were sent to the inmates to help them locate the deliveries, with some mobile and drone forensics aiding the prosecution team in their case. Both of these and more in this week's report.

As always, if you have comments or feedback, want to join in the discussion in our slack group, or find out how we capture all 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.

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.

Battlefield Operations	Priority
Continued UAV incidents involved in conflict between Azerbaijan and Armenian troops	**P2**

Summary

A number of incidents have been attributed to UAV use by Azerbaijan in their offensive against Armenian-held territory. So far, none of the current reports indicate quadcopter or COTS use; however, previous surveillance artefacts the month prior have pointed towards quadcopter use.

Note: This report contains battlefield footage that some might find upsetting.

Overview

After weeks of drone surveillance and proxy incidents, an offensive has been launched regarding Armenian-held territory claimed by that of Azerbaijan. Weaponised drone strikes against towns, kamikaze drones against troop positions and anti-tank/artillery actions have been enabled by Azerbaijani drones.

Armenia has claimed 150+ downings of adversary drones, however reports are unclear if these figures include kamikaze-based drones or the method used to destroy them.

Multi-Incident Analysis:

Armenian Ministry of Defense shares video of downed AN-2 Azerbaijani drone

- https://www.almasdarnews.com/article/moment-azerbaijani-drone-crashes-after-being-hit-by-armenian-forces-video/

Armenia air defence shoots down Azerbaijani drone in north east Artsakh

- https://en.armradio.am/2020/10/02/azerbaijani-aircraft-and-drone-shot-down-by-armenian-forces/

Azerbaijan drone crashes in Parasad county, Iran

- https://english.alarabiya.net/en/News/middle-east/2020/10/13/Unidentified-drone-lands-in-Iran-near-Azerbaijan-border-Official-

Drone Wars: In Nagorno-Karabakh, the future of warfare is now (commentary)

- https://www.rferl.org/a/drone-wars-in-nagorno-karabakh-the-future-of-warfare-is-now/30885007.html

The key to Armenia's tank losses: the sensors, not the shooters (commentary)

- https://rusi.org/publication/rusi-defence-systems/key-armenia-tank-losses-sensors-not-shooters

Turkish drone power displayed in Nagorno-Karabakh conflict (commentary)

- https://www.voanews.com/middle-east/turkish-drone-power-displayed-nagorno-karabakh-conflict

Threat Actor Profile: Azerbaijani Army

Motivation and Goals:

- To conduct ranged, loitering and weaponised attacks via drones against enemy positions
- To record and publicise drone attack footage for propaganda and/or patriotism

Tactics, Techniques and Procedures:

- Use of unmanned systems to conduct surveillance, reconnaissance and destructive combat missions
- Use of unmanned systems to cause causalities in battlefield
- Using 'kamikaze' drones to perform dive attacks against armoured vehicles and troop positions
- Sourcing military-based drone systems and technology from various countries

Recorded Use of Drone/Equipment:

- Turkish-made Bayraktar TB2
- Orbiter 1K UAV
- Israeli-made HAROP Azeri
- Israeli-made Aerostar
- Antonov An-2

This threat actor profile is currently in development. We'd like to hear from you if you have observed other TTPs or signature uses of unmanned systems by this actor.

Intrusion and Trespass	Priority
Ex-inmate arrested with intent to deliver contraband via drone into Fort Dix Correctional Facility	**P2**

Summary

Three men were arrested for taking part in the planning of several drone deliveries into Fort Dix prison between 2018-2019.

Overview

Security officers from Fort Dix Correctional Facility spotted a drone with a fishing line hovering above the rooftop of the prison and found a bag of tobacco, cell phone, cell phone chargers, USB charging cables and an inmate within the area. An in-depth investigation was conducted and three men were suspected of participating in the drone delivery, of which, one was an ex-inmate who was released a month ago. Communication devices led the police to the conversations the culprits had with the inmates and several aerial photos of the prison. More evidence was found in the home of the ex-inmate and the arrest was made.

Analysis

In most cases, recurring drone incidents are caused by a repeating offender or organised group. In the case of Fort Dix Correctional Facility, two of the offenders have made several drone deliveries before and was fed with more information when an ex-inmate joined them after his release. Being an ex-inmate, the offender had insider knowledge on the security protocol of the prison and its vulnerabilities. This information would have given the offenders a huge advantage in committing the crimes with a greater degree of success.

Fort Dix has experienced previous cases of contraband drone deliveries before and is part of their security protocol to keep a lookout for aerial infringements. Illegal prison deliveries via the use of drones reflect the growing adaptation and innovation of individuals and criminal groups. Without any counter drone systems installed, threat actors will always try their luck to send deliveries into prisons as drone deliveries impose a low risk of them being apprehended by distance (away from the area of crime) and wireless transmission.

Threat Actor Profile: Local Prison Disruptors

Motivation and Goals:

- To deliver contraband safely and undetected across the prison walls to supply incarcerated individuals

Tactics, Techniques and Procedures:

- Use of unmanned systems to separate the distance and risk between operators and contraband payloads
- Use of unmanned systems to conduct reconnaissance and delivery missions
- Use of unmanned systems to overcome physical and personnel security barriers and controls

- Sourcing cheap and available Commercial-Off-The-Shelf (COTS) drones for one-way flights
- Bypassing No-Fly-Zones (NFZ) and restricted airspace by modding and device rooting
- Self-taught in unmanned and contraband-delivery UAS flights and operations
- Using small COTS drones to drop contraband (cellphones, narcotics, weapons ~<2kgs) onto prison grounds, often with purchased or home-made dropping mechanisms
- Utilising counter-forensics techniques by removing SD cards, disabling caching, destroying serial info and disabling the Return-to-Home functionality

Recorded Use of Drone/Equipment:

- Quadcopters, Multi-rotors
- PGYTECH Air Dropping System
- Homemade contraption with household items (spork, sewing string, fishing string)

Recorded Contraband/Crime:

- Narcotics (cannabis, marijuana, tobacco, steroids)
- Communication devices (cell phones, SIM cards, batteries)
- Equipment (syringe)
- Weapons (saw blade, screwdrivers)

Recommendations

DroneSec recommend for prisons and areas that require a no-drone-zone policy to have a drone threat management Standard Operating Procedure (SOP) or incident response plan in place. This should help 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 and categorised. 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.

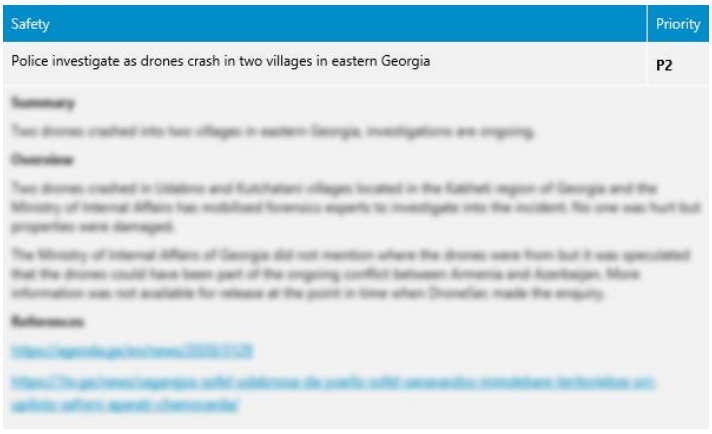
Finally, correctional facilities that are in Counter-Drone-denied environments (whether regulatory or financially) should seek detection systems that do not seek to necessarily mitigate but do provide tracking and post-incident analysis capabilities.

References

https://hudsoncountyview.com/feds-jersey-city-man-tried-to-use-drones-to-smuggle-tobacco-cell-phone-chargers-into-jail/

Intrusion and Trespass	Priority
More mysterious drone flights near police post raises concerns	P2

Figure 1 - Can't see this report? Contact info@dronesec.com to unlock.



Safety	Priority
Police investigate as drones crash in two villages in eastern Georgia	P2

Figure 2- Can't see this report? Contact info@dronesec.com to unlock.

1.3. NEWS AND EVENTS (P3)

Arab Coalition air defence destroys two explosive-filled drones launched by Houthi militia

https://www.arabnews.com/node/1746741/saudi-arabia

https://www.arabnews.com/node/1747151/saudi-arabia

Traffic halted briefly at Spain's Tenerife Norte-Los Rodeos airport due to alleged drone sighting

https://www.eldia.es/sucesos/2020/10/11/dron-paraliza-trafico-aereo-rodeos/1116288.html

Man charged for shooting drone on approved works on electrical towers, United States

https://times-herald.com/news/2020/10/drone-struck-man-charged-with-shooting-15k-device

The Spanish Civil Guard has discovered a narcodrone carrying 4kg of drugs on Moroccan border

https://www.lasprovincias.es/sociedad/guardia-civil-detecta-20201001200637-nt.html

Californian man charged for falsifying drone registration certificates and waivers for drone show

https://www.suasnews.com/2020/10/california-man-indicted-for-fraud-and-identity-theft-related-to-a-drone-show/

Queensland firefighters issue notice on no-fly-zone for drones in Kooralbyn fire, Brisbane

https://www.ntnews.com.au/breaking-news/drone-operators-warned-off-by-queensland-firefighters-as-they-battle-bushfire-south-of-brisbane/news-story/8538ec0cff565752595473b189c2877a

Gull attacks and crashes DJI Matrice M200 drone during approved roof inspection

https://assets.publishing.service.gov.uk/media/5f5a04258fa8f51067771008/DJI_Matrice_M200_UAS_registration_na_10-20.pdf

1.4. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P4)

US DoJ forecast increase in Counter-UAS protection activities and criminal enforcement actions

https://www.justice.gov/opa/pr/department-justice-forecasts-increase-counter-unmanned-aerial-systems-c-uas-protection

DJI expresses disappointment on ban of DJI drones with trade protectionism for 'blue sUAS'

https://dronedj.com/2020/10/07/another-doi-push-toward-made-in-us-drones-and-against-china/

Singapore imposes drone theory, practical exams and proficiency checks for drones over 1.5kgs

https://www.straitstimes.com/singapore/want-to-fly-drones-above-15kg-undergo-training-and-pass-an-exam

FAA submits final review of rules on "Remote ID" and "operations of drones over people"

https://www.aopa.org/news-and-media/all-news/2020/october/09/drone-rules-on-final-approach

Drone manufacturers push for legal drone fly zones in India for testing purposes

https://timesofindia.indiatimes.com/city/hyderabad/push-for-dedicated-fly-zones-to-test-drones/articleshow/78610430.cms

Force Protection India 2020 event highlights that UAVs stand out against other threats

https://www.newindianexpress.com/nation/2020/oct/10/drones-stand-out-among-other-threats-in-their-destructive-potential-lt-gen-sk-saini-2208494.html

Turkey begins to rival China in military drones (commentary)

https://asia.nikkei.com/Politics/International-relations/Turkey-begins-to-rival-China-in-military-drones

How Turkey outclassed the UK with their own technology to develop one of world's most lethal drones (commentary)

https://eurasiantimes.com/how-turkey-outclassed-the-uk-with-their-own-technology-to-develop-one-of-worlds-most-lethal-drones/

Drones stand out among other threats in their destructive potential (commentary)

https://economictimes.indiatimes.com/news/defence/drones-stand-out-among-other-threats-in-their-destructive-potential-army-vice-chief/articleshow/78589359.cms

As drones become more common, privacy concerns arise (commentary)

https://www.wvxu.org/post/drones-become-more-common-privacy-concerns-arise#stream/0

1.5. COUNTER-DRONE SYSTEMS (P4)

Isreali MCTECH wins tender to deliver counter-drone system to African country

https://www.israeldefense.co.il/en/node/45496

AeroDefense announces lightweight Smart Drone Detection for urban cities

https://www.businesswire.com/news/home/20201008005182/en/AeroDefense-Solves-Urban-and-Airport-Drone-Detection-Challenges-with-Small-Discreet-Antenna-and-Fiber-Deployment

Echodyne releases EchoGuard and RadarHub for urban CUAS detection

https://www.echodyne.com/news/echodyne-expands-product-line-to-meet-growing-demand/

US Department of Defense to release joint counter drone strategy and align future technologies

https://www.army.mil/article/239593/joint_counter_suas_strategy_to_address_need_for_improved_technology

Chile awards Israeli Skylock with the supply of three detect and mitigate counter drone systems

https://www.unmannedairspace.info/counter-uas-systems-and-policies/chile-selects-skylock-counter-drone-solution-to-locate-mitigate-and-capture-unauthorised-drones/

US Army solidifies requirements to counter small drones (commentary)

https://www.defensenews.com/digital-show-dailies/ausa/2020/10/12/us-army-solidifies-requirements-to-counter-small-drones/

India's airports remain at risk as no counter drone systems installed to mitigate drone incursions

https://www.timesnownews.com/india/article/indias-airports-remain-at-risk-nothing-done-to-tackle-threat-from-drones/666460

Ascent Vision tests X-MADIS counter drone system at Camp Grafton Training Center

https://ascentvision.com/avt-conducts-counter-uas-system-testing-at-cgtc/

1.6. UTM SYSTEMS (P4)

Kittyhawk releases Air Control, a UTM platform for enterprise customers

https://dronedj.com/2020/10/08/kittyhawk-announces-air-control-enterprise-driven-utm-platform/

1.7. INFORMATIONAL (P5)

Drone used to monitor and bust drug deal, China

https://www.bbc.com/news/technology-54526515

UK military to use i9 drones for breaching operations instead of soldiers

https://i-hls.com/archives/104357

North Yorkshire police employ drones to search for missing man, United Kingdom

https://www.thenorthernecho.co.uk/news/18776564.police-use-drone-hunt-missing-joseph-cafferkey/

Ukraine expresses interest in buying Turkey's Bayraktar TB2 drones

https://ahvalnews.com/turkey-defence-industry/ukraine-considering-buying-turkeys-bayraktar-drones-turkish-media

Serbia looks to buy Turkey's Bayraktar TB2 drones from proven battlefield effectiveness

https://dronedj.com/2020/10/07/serbia-looks-to-buy-turkish-drones-strengthening-relations/

US Army releases RFI for Signal Intelligence (SIGINT) payload for MQ-1C drone

https://beta.sam.gov/opp/ac885a2995694e67ab25830924eec044/view?keywords=intelligence&sort=-modifiedDate&index=opp&is_active=true&page=1

AeroVironment secures USD$8.4M sale of Puma 3 AE drones for an allied nation

https://insideunmannedsystems.com/aerovironment-secures-8-4-million-puma-3-ae-unmanned-aircraft-systems-foreign-military-sales-contract-award-for-u-s-ally/

United States to sell more drones and missiles to Taiwan (commentary)

https://www.aljazeera.com/news/2020/10/14/us-plans-to-sell-more-drones-missiles-to-taiwan-report

STM to deliver 2kg kamikaze drone, Alpagu, to Turkish military by December 2020

https://www.defenseworld.net/news/27980/Kamikaze_Drone__Alpagu__to_be_Deployed_with_Turkish_Security_Forces_by_Year_end#.X35vp2gzaUk

1.8. DRONE TECHNOLOGY (P5)

RAF tests swarm loaded with BriteCloud electronic warfare decoys to overwhelm radar systems

https://www.thedrive.com/the-war-zone/36950/raf-tests-swarm-loaded-with-britecloud-electronic-warfare-decoys-to-overwhelm-air-defenses

Ciconia successfully demonstrates collision avoidance system on simulated helicopter and drone

https://www.unmannedairspace.info/latest-news-and-information/ciconia-mid-air-conflict-management-system-tested-between-helicopter-and-drone/

GPS denied drone to be trialled in South Africa with Hovermap's LIDAR sensor

https://www.miningweekly.com/article/gps-denied-drone-trialled-in-south-africa-with-keen-eye-on-underground-mine-mapping-2020-10-09

India' stealth strike bomber drone "Ghatak" revealed in Indian Institute of Technology

https://eurasiantimes.com/indias-most-secretive-stealth-drone-project-uncovered-as-it-aims-to-counter-dassault-boeing-northrop-ucavs/

Defendtex awarded AUD$2.1M for development of drone platform by Defence Innovation Hub

https://www.minister.defence.gov.au/minister/melissa-price/media-releases/innovation-hub-invests-28-million-australian-industry

Turkey unveils new TUSAS Aksungur combat drone with SIGINT and anti-submarine capabilities

https://jamestown.org/program/turkey-makes-new-advances-in-land-and-naval-warfare-with-introduction-of-aksungur-asw-drone/

Project GAUSS conducts satellite navigation drone operation with Galileo and EGNOS

https://www.suasnews.com/2020/10/project-gauss-performs-first-flight-campaigns-with-drones-to-assess-the-capabilities-of-galileo-and-egnos/

Russia's helicopter gunships to get launch-capable mini suicide drones from missile tubes

https://www.uasvision.com/2020/10/14/russias-combat-helicopters-to-get-suicide-drones/

1.9. SOCIALS (P5)

Portuguese military uses drone to surveil before assault on 3R rebels in Central African Republic

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

Crowded Space drones secure certification for use of drones in surveillance

https://www.linkedin.com/posts/crowdedspacedrones_uk-compliance-drones-activity-6722070788670926848-RP4W

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) UAS 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.

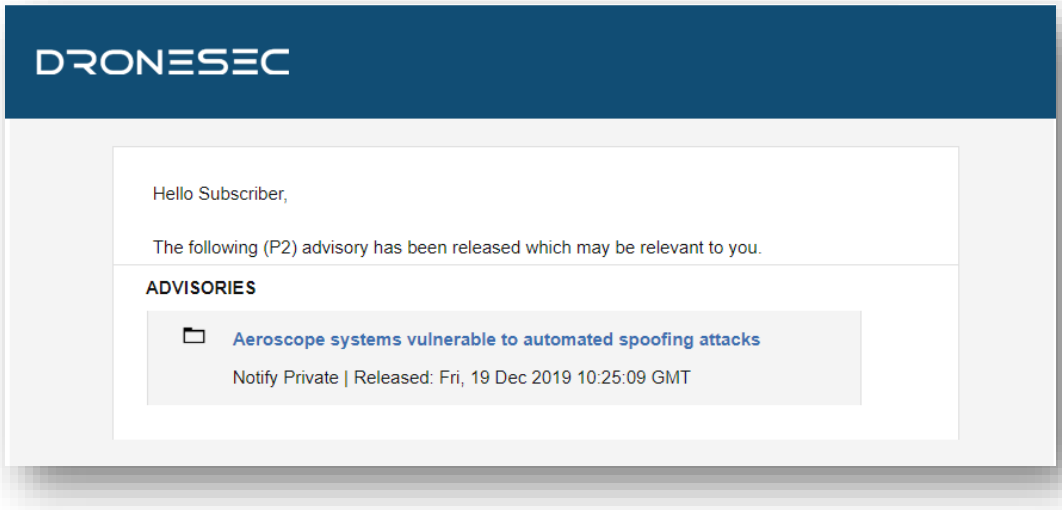


Figure 3 - A threat notification specific to a Notify customer's listed keywords.

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 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.