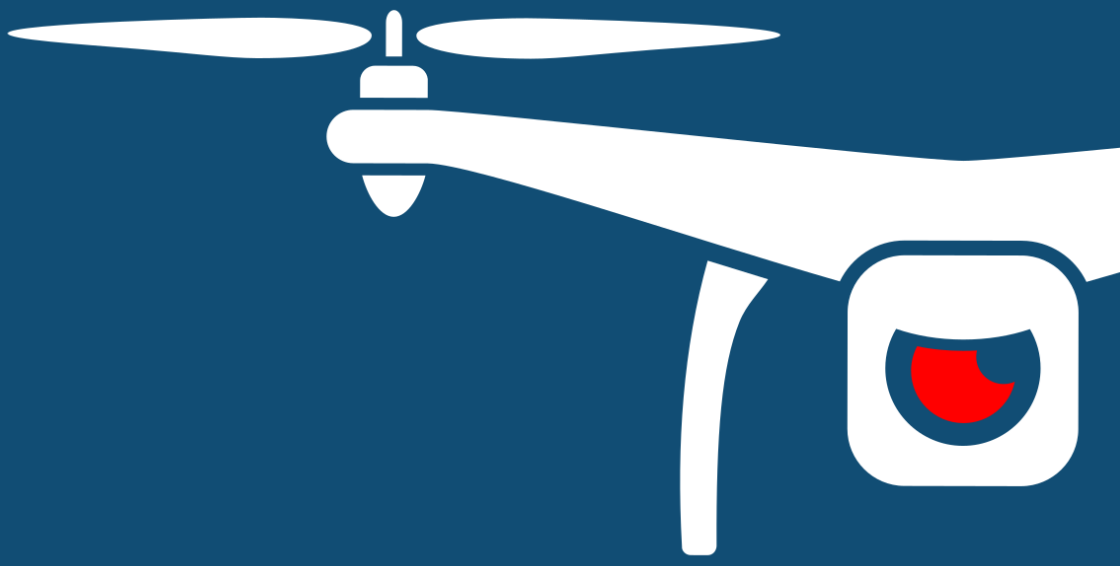
DRONE SEC
A Privasec COMPANY

NOTIFY ISSUE #48 (PUBLIC)

WEEKLY THREAT INTELLIGENCE

11 November 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

This week, DroneSec is included in the cyber and data security section of the threat intel report. At the AISA 2020 and World of Drones and Robotics Congress 2020 conferences, we announce some major cyber-security vulnerabilities, issues and misconfigurations specifically affecting the drone, UTM and C-UAS space.

Over the past year several security findings were observed by our threat intel analysts but not disclosed in these reports. Instead, they were guided through remediation within client engagements, responsible disclosure process, bug bounty programs or through government agencies. As a result, we've summarised (and anonymised) some of the highest impact findings of what we've observed to share these with the public. Currently, a large part of the unmanned ecosystem is vulnerable to information leakage, fleet takeovers and even in some cases, remote disabling of Counter-Drone systems.

In the coming weeks, we'll be releasing more specific guidance to vendors, developers and operators in order to better protect their systems against the specific vulnerabilities we have identified. In the meantime, the presentation will be available in the form of a write-up when the conferences come to a close.

On to the other highlights of the week: an incredibly insightful look and interesting read into Fort Benning military operations with squad UAS and Counter-UAS – one of the key strengths of Notify is that we pick up *everything* related to UAS security, as long as it's publicly available. In the Armenia-Azerbaijan conflict, we start seeing more Commercial-Off-The-Shelf (COTS) drones appearing amongst militants – not just the big military drones playing part of the action.

In the USA we observe another medical helicopter interference by rogue drone, and a potential collision with a light aircraft in the Netherlands which involved the Royal Netherlands Air Force to assess damage before making a controlled landing.

In terms of COTS drone modifications, footage has emerged of an 8km height managed with modified batteries in Greece, and an 18km cross-border flight between Singapore and Indonesia, also using modified batteries and range extenders. These artefacts should give law enforcement and security operators a better understanding of the realistic capabilities of modified COTS systems, and the potential range and height they're dealing with. Similarly, it is important to document the technology enabling these operations to identify potential or future activities in an area.

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.

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. 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.

Safety	Priority
Rogue drone delays first responders' medical helicopter from landing, Columbus	P2

Figure 1 - Can't see this report? You're viewing the PUBLIC edition of DroneSec Notify.

Safety	Priority
Manned aircraft returns for landing after possible collision with drone, Netherlands	**P2**

Summary

A two-passenger plane heard a loud bang in mid-air and made a precautionary landing, discovering that the plane's nose and propeller was damaged.

Overview

While flying at an altitude of 600metres near Aalst and Veen in Netherlands, both pilots in a sports plane heard a loud bang and felt a collision on their aircraft. Ensuring safety, the pilots took the plane down for landing at the nearby Eindhoven Airport. The pilots conducted a landing gear inspection with the help from an Apache helicopter from the Royal Netherlands Air Force before a landing occurred.

After proper inspection, the nose of the aircraft and its propeller was damaged, probably by a drone as aviation investigators ruled out bird strike. The drone and its operator were not found.

Analysis

This incident clearly reflects the environment and behaviourism of errant drone operators commonly observed nowadays - the ability to conduct unauthorised flights without much risk of being apprehended. It is increasingly difficult to trace down drone owners without registration of drones where users my mod their drone systems. In addition, much cannot be done by law enforcement agencies to detect and deter such acts from happening as drones are easily available, cheap in contrast to counter drone or drone detection systems.

It is important that drone operators are cognisant of these aviation laws and the consequences of their actions as a near miss or a direct hit could result in potential fatalities. Flight restriction over populace and aerodromes are set in place to prevent any possible drone-related collisions. Studies have shown that a direct impact from a drone deals an extensive amount due to the drone's hard exteriors as compared to other forms of collisions such as bird strikes.

Recommendations

Operators should aim to keep themselves up to date and relevantly trained before operating a drone. Also, they should be updated with bulletins explaining any new rules or procedures as they become available. Rules on drone operation can be found online in the local government aviation websites and mobile applications for the convenience of operators. Organisations with drone operations should aim to keep themselves and their personnel up to date and relevantly trained before operating a drone. It is the responsibility of drone operators to be sufficient trained, certified and updated with the latest regulations, procedures and NOTAMs as soon as they become available.

References

https://www.politie.nl/nieuws/2020/november/11/1-gewichtsgrug-botst-vermoedelijk-met-drone.html

Figure 2 - Can't see this report? You're viewing the PUBLIC edition of DroneSec Notify.

Intrusion and Trespass	Priority
Yuma Sector arrests two for picking up narcotics dropped from a drone crossing national borders	**P3**

Summary

Two adults were arrested after they were spotted picking up packages dropped off from a drone that entered from Mexico.

Overview

Yuma Sector Customs and Border Protection officers detected a drone making multiple trips between the Mexico-United States border near San Luis and investigated the vicinity of the drop off point. They spotted an adult male and female picking up the packages and an arrest was made. The packages contained narcotics, methamphetamine, and further checks on the residence of the duo resulted in a seizure of another 11kg of narcotics and a handgun. The drone and its operator were not found.

Analysis

In this incident, the act could have been performed by a repeating offender or organised group as the drop off point seems to be scouted beforehand and the trips were well coordinated. In addition, DroneSec is starting to see more drone deliveries across national borders and prisons carrying heavier payloads. Offenders and organised crime groups may have realised that law enforcement agencies are starting to take note of illegal deliveries and are innovating new methods to avoid detection. One of the ways to reduce the risk of losing contraband and getting caught, if the drone was seized, is to overload the unregistered drones or purchasing a more costly but high weight-capacity drone to reduce the number of delivery runs.

The availability of COTS drones makes it an easily accessible tool. Without too much risk of the operator being apprehended as both entities are separated by distance and wireless transmissions, coupled with a low skill barrier for a successful drone operation, such method of deliveries becomes more lucrative to offenders. Offenders for such acts tend to get away easily as most crime happen in areas where drone detection or counter-drone systems cannot be implemented effectively (cost and coverage wise) to mitigate the threat.

Recommendation

The San Luis border patrol officers have encountered illegal drone deliveries since 2015 and they have a sound Standard Operating Procedure (SOP) and security management plan for drone infringements. Yuma Sector may possibly have a drone detection system installed as well. The incident drone was detected making multiple runs which gave the officers an opportunity to catch the suspects red handed.

It is important for law enforcement agencies to have a standard operating procedure (SOP) which aid to govern the process, people and methodology in handling a drone, collecting evidence and responding to potential operators in a pre-determined radius around the protected grounds. Likewise, all sightings and detections should be logged and categorised. Successful incidents often see offenders becoming lax with their approach and utilising the same take-off/landing points as before. However, as these suspects were arrested, the Yuma Border Patrol can expect drone operators to take different paths of ingress to avoid detection.

In the event of a seized drone, event analysis from the drone data and video footage and recognising patterns and trends (such as origin of flight, time of day etc) may help provide the modus operandi of rogue groups and may aid in the arrest of the operator.

References

https://www.thedesertreview.com/border_patrol/yuma-agents-detect-cross-border-drone-smuggling-narcotics/article_73938224-22a7-11eb-89ea-bb89ed7d0f24.html

https://kyma.com/news/2020/11/10/two-arrested-after-drone-drops-packages-of-meth/

1.3. CYBER AND DATA SECURITY (P2)

DroneSec reveal remote hacking takeovers of drone, UTM and Counter-Drone systems

https://conference.aisa.org.au/risk-cyber-week/agenda

https://www.worldofdrones.com.au/program

Hexagon and NovAtel introduce GRIT, an anti-jamming and spoofing firmware update for drones

https://www.unmannedsystemstechnology.com/2020/11/new-gnss-anti-jamming-spoofing-technology-released/

Easy Aerial launches tethered drone with constant un-jammable data communication link

https://dronedj.com/2020/11/06/easy-aerial-launches-its-sams-t-mini-drone-monitoring-system/

1.4. NEWS AND EVENTS (P3)

Civilians injured in a drone and mortar attack by Houthi terror group

https://www.arabnews.com/node/1758971/middle-east

Afghan troops capture weaponised drone amongst weapon cache in a Taliban raid

https://menafn.com/1101097128/Afghan-troops-capture-a-Taliban-weaponized-drone-in-south

Arab Joint Coalition Forces destroyed bomb-laden drone launched by Houthi against civilians

https://english.alarabiya.net/en/News/gulf/2020/11/09/Arab-Coalition-destroys-drone-launched-by-Yemen-s-Houthis-toward-Saudi-Arabia

Israeli Defence Forces downs Lebanese Hezbollah drone intruding into Israeli airspace

https://www.timesofisrael.com/military-says-it-downed-hezbollah-drone-that-entered-israeli-airspace/

Garmin to investigate use of technology in Bayraktar TB2 drones in Armenia-Azerbaijan conflict

https://en.armradio.am/2020/11/04/garmin-company-says-will-investigate-use-of-its-technology-in-turkish-drones/

Four Azerbaijani drones shot down in Armenia within 1.5 hours

https://en.armradio.am/2020/11/04/fourth-azerbaijani-drone-shot-down-in-armenias-gegharkunik/

Azerbaijani Bayraktar TB2 drone shot down by Armenian air defence unit

https://defence-blog.com/news/armenia-claims-it-shot-down-azerbaijani-bayraktar-tb2-combat-drone.html

Azerbaijan releases footage of drone attack against Armenian air defence vehicle

https://defence-blog.com/news/army/azerbaijani-drone-blows-up-armenian-modern-air-defense-system.html

Singaporean man fined SGD $16,000 for flying drone over restricted areas and above height limit (update)

https://www.straitstimes.com/singapore/courts-crime/man-fined-16000-after-flying-drone-near-gombak-base-multiple-times

FAA places no-fly-zone over Joe Biden's home in Delaware

https://www.businessinsider.com.au/faa-restricts-airspace-over-bidens-home-in-delaware-2020-11

Russia exercises long-range radio-electronic warfare to supress enemy radio signals of up to 5,000km, including drones

https://thebarentsobserver.com/en/security/2020/11/russia-exercises-long-range-strategic-radio-jamming-kola

US Air Force purchases 57 DJI drones for counter-measure training, sparking privacy concerns

https://www.wsj.com/articles/air-force-purchase-of-chinese-drones-spurs-security-concerns-11604322017

1.5. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P3)

EASA updates its "Easy Access Rules for UAS" publication

https://www.unmannedairspace.info/latest-news-and-information/easa-updates-its-easy-access-rules-for-uas-publication/

Results of European UAS operations and risk survey published

https://www.unmannedairspace.info/latest-news-and-information/results-of-european-uas-operational-survey-published/

India's Civil Aviation to drive recruitment for commercial drone pilot

https://www.commercialdroneprofessional.com/india-launches-drone-pilot-training-and-recruitment-drive/

Department of Defense Counter-Unmanned Aircraft Systems (Congressional Research Service)

https://fas.org/sgp/crs/weapons/IF11426.pdf

The Mafia is using drones for drug shipments between Morocco and Ceuta (commentary)

https://notify.dronesec.com/storage-protected/W43Ndkqklf0YiGvyAJ0M8GK1dOs9VkZS4qLztWHi.pdf

Azerbaijan-Armenia conflict: Israeli 'kamikaze' drones wreak havoc on Karabakh (commentary)

https://www.middleeasteye.net/news/azerbaijan-armenia-israel-kamikaze-drones-nagorno-karabakh-shushi

Pakistan arming Kashmir-centric terrorist groups with drones (commentary)

https://www.indiablooms.com/news-details/N/66581/pakistan-arming-kashmir-centric-terrorist-groups-with-drones-think-tank.html

Distributed Extended Kalman Filtering Based Techniques for 3-D UAV Jamming Localization

https://www.mdpi.com/1424-8220/20/22/6405/pdf (PDF Document)

Evolving the Infantry Brigade Combat Team's Cavalry Squadron to Win the Recon Fight

https://www.benning.army.mil/armor/eARMOR/content/issues/2020/Fall/4BromanPartII20.pdf (PDF Document)

1.6. COUNTER-DRONE SYSTEMS (P4)

Tests of several drone detection systems by Germany's air navigation provider favours mixed sensors for employment

https://www.unmannedairspace.info/counter-uas-systems-and-policies/first-results-from-germanys-drone-detection-tests-favour-mix-of-different-sensor-technologies/

Department 13 delivers MESMER counter drone system to South East Asian country

https://www.geospatialworld.net/news/department-13-delivers-counter-drone-technology-to-another-south-east-asian-government/

Citadel Defense updates CUAS systems with AI to better response time against drone threats

https://www.businesswire.com/news/home/20201110005152/en/

University of Technology Sydney and DroneShield demonstrate new optical system for C-UAS

https://www.unmannedairspace.info/counter-uas-systems-and-policies/droneshield-uts-announce-new-ai-based-optical-drone-detection-system/

South Korea installs Black Sage drone detection system at Incheon International Airport

https://blacksagetech.com/repository/black-sage-contributes-to-successful-drone-detections-at-incheon-international-airport

Rafael integrates Sky Spotter's passive early warning system into Drone Dome CUAS system

https://www.unmannedairspace.info/counter-uas-systems-and-policies/rafael-adds-sky-spotter-sensor-to-its-drone-dome-c-uas-network/

Drone Defence awarded £378,000 grant for detection capabilities: UKR&I Future Flight Challenge

https://www.dronedefence.co.uk/drone-defence-secures-future-flight-challenge-fund-grant/

1.7. UTM SYSTEMS (P5)

Consortium presents 2-years examination on critical issues on UTM Comms in Singapore

https://www.unmannedairspace.info/latest-news-and-information/singapore-consortium-presents-findings-of-18-months-utm-programme-development/

DroneCloud awarded £500,000 to lead Project Rise – BVLOS flight trials and integration of UTM with Drone Management Software

https://www.unmannedairspace.info/latest-news-and-information/project-rise-addresses-utm-in-bvlos-flight-trials-as-part-of-uk-future-flight-challenge-project/

South Africa's air nav, ATNS, outlines UTM framework as part of ATM integration

https://www.unmannedairspace.info/uncategorized/south-africa-outlines-its-national-utm-concept-as-a-subset-of-the-atm-system/

Are drones and flying taxis the future of aviation? (commentary)

https://newseu.cgtn.com/news/2020-11-05/Are-drones-and-flying-taxis-the-future-of-aviation--V9tpg618Bi/index.html

1.8. INFORMATIONAL (P4)

UK Police reveal extensive use of drones for operations, 675 times since January 2020 (Update)

https://www.urbanairmobilitynews.com/first-responders/uk-police-forces-increase-use-of-drones-as-just-constabulary-have-helped-secure-47-arrests-and-successfully-located-11-missing-people-this-year/

Mesa County PD finds lost hunter with help from thermal drone

https://www.gjsentinel.com/news/western_colorado/drone-finds-lost-hunter-on-friday/article_a844a65a-1e1b-11eb-8fb2-e75898337bf2.html

Russia successfully trials target drone helicopter created by CSTS Dinamika

https://www.defenseworld.net/news/28220/Russia_Develops_New_Rotary_Wing_Target_Drone

£33 million awarded to fund drone swarming and aviation technologies in the UK

https://www.gov.uk/government/news/drones-to-fight-fires-and-deliver-covid-19-supplies-are-first-to-receive-share-of-over-33-million-government-funding

Drone and K9 unit assist Police in finding runaway driver under influence, California

https://www.sacbee.com/news/local/crime/article247087997.html

Vantage awarded USD $2.5M to design micro drone for the U.S. Army

https://defence-blog.com/news/army/pentagon-awards-new-contracts-to-vantage-for-reconnaissance-systems.html

Autel Robotics partners DroneSense for public safety operations on EVO drones

https://www.suasnews.com/2020/11/autel-robotics-and-dronesense-partner-to-enable-advanced-public-safety-uas-operations/

1.9. DRONE TECHNOLOGY (P5)

DJI launches the 249 gram DJI Mini 2 drone with 4K camera and OcuSync Transmission

https://www.dji.com/newsroom/news/dji-mini-2

Hyundai Motors to unveil unmanned cargo aircraft in 2026

https://www.kedglobal.com/newsView/ked202011080001

A.Drones and Athlon Avia to develop stealth loitering kamikaze drones

https://defence-blog.com/news/army/ukrainian-companies-develop-stealth-combat-drones.html

Stealth Technologies partners Planck Aerosystems to develop vision-based drone landing on moving platforms without GPS

https://www.defenceconnect.com.au/air-sea-lift/7139-stealth-technologies-partners-with-planck-aerosystems

Blue Bear demonstrates simultaneous remote launching of drones for autonomous operations

https://www.aerospacetestinginternational.com/news/drones-air-taxis/blue-bear-demos-simultaneous-drone-launch-capability.html

1.10. SOCIALS (P3)

COTS drone seen amongst armed military war fighters in Stepanakert, Armenia

https://twitter.com/khalfaguliyev/status/1325098476338810881/photo/1 (image)

https://t.me/karabah_news/3229 (video)

Video of Azerbaijan drone shot down by Armenian small arms fire

https://www.instagram.com/tv/CHRzoOqnOPi/

Operator flies DJI Mavic Pro Platinum at height of 8,005m with modified batteries, Greece

https://www.youtube.com/watch?v=lOtRQJdGv1I&fbclid=IwAR1eJqzOje0P5DFORyKXTDN26U_4ldh1cs4zKrob0AcDWKENFHpoTxnXjvo

Operator in Singapore flies modified DJI drone 18km across border to Indonesia's Riau Islands using 11740mah battery and Itelite Nanosync antenna

https://www.youtube.com/watch?v=S0uoMEk0HxA

DroneShield CEO Oleg Vornik on UAS Threating safety, security & privacy (Podcast)

https://www.youtube.com/watch?v=tMH8gX0LyBA

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.

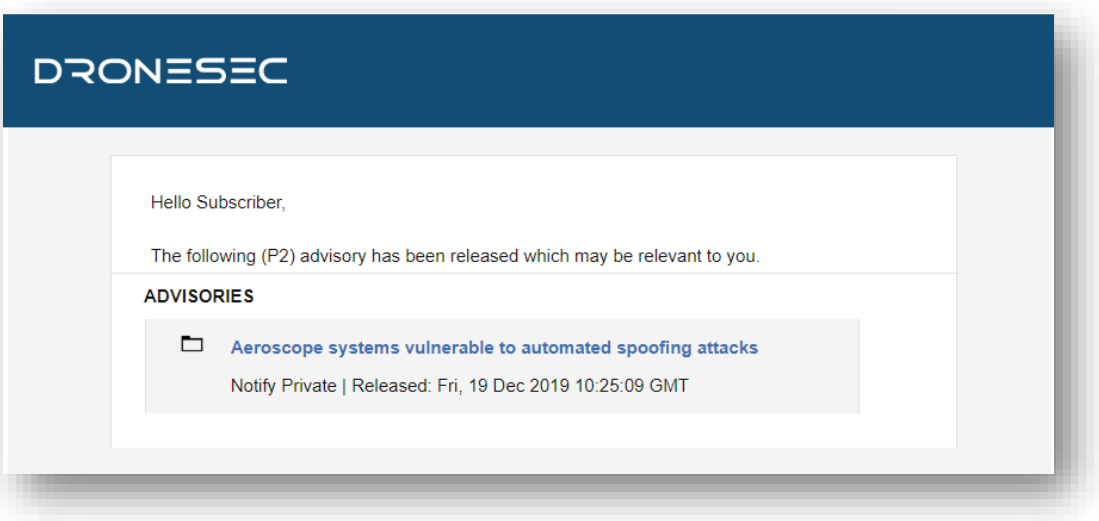


Figure 3 - A threat notification specific to a Notify customer's listed keywords.

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 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.