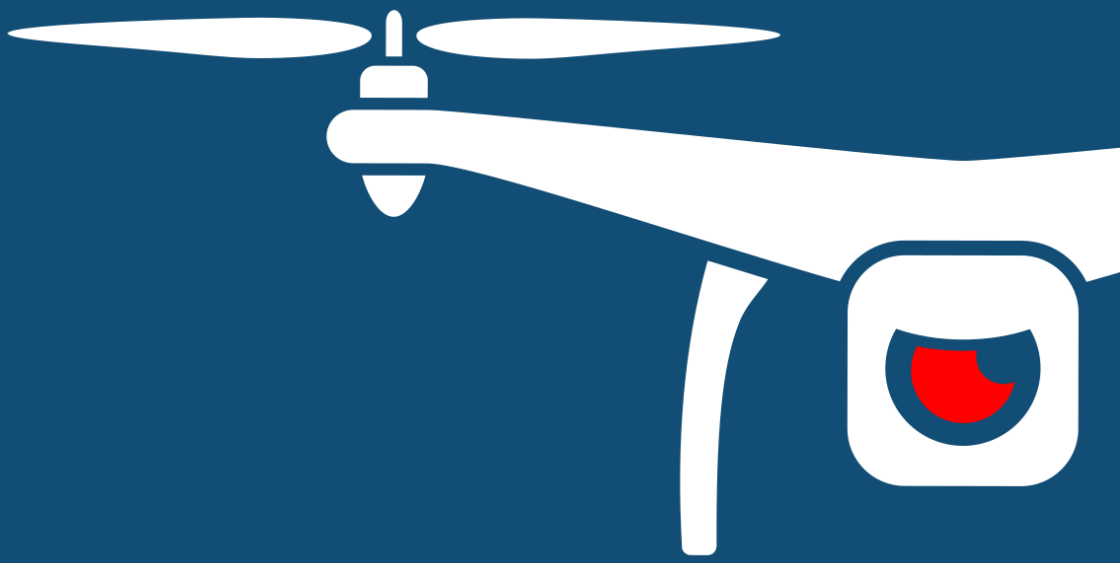
DRONE SEC
A Privasec COMPANY

NOTIFY ISSUE #40 (PUBLIC)

WEEKLY THREAT INTELLIGENCE

16 September 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

A small reflection today as our system recorded our 100th report released to the public. Likely not something to be joyful about, but a considerable reflection on the industry in 2020 nevertheless.

Prisons and correctional facilities are currently inundated by drones dropping contraband into the premises. A huge item of interest this week is the USA Department of Justice and Board of Prisons audit-report that focuses on some incidents, recommendations and guidance as to identifying, documenting and preventing future sUAS threats. The report is comprehensive and echoes various Law Enforcement concerns around the globe, that they are in no position to respond to the threat.

Even within Australia, the WA Police have mentioned that not only can they not intercept a sUAS being flown by a nefarious operator, but in some cases the laws prevent them from even tracing the device to a place or the person operating the device. Something we've always talked about in this space is the need for industry maturity and matching that of the laws. Audit reports by that of the BOP bring up real issues faced by those across the globe and it can only be hoped it paves the way not just for the USA but elsewhere.

On the cyber-security front, Kittyhawk released a whitepaper for guidance on secure drone programs, underlying infrastructure and control systems. A key note is to have systems undergo a 'red team' or penetration test by an independent company to put it through a true-test of what your systems might undergo by less-law-abiding users across the internet. A true testament to the state of drone security, cyber-specific vulnerabilities will continue to be a key focus on the unmanned environment for years to come. All these and more in this week's report.

The public links to go live for the Global Drone Security Network (GDSN) event **this Friday 1900 September 18th** will be published shortly so keep an eye on your inbox and social channels. We look forward to you joining us then and thank you to all those that have already taken part.

As always, if you have comments or feedback, or want to join in the discussion in our slack group, 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.

Intrusion and Trespass	Priority
Failed drone delivery into Mississippi prison leads to two men arrested with drone forensics	**P2**

Summary

A DJI Phantom 3 drone was caught in a net above the perimeter fence of the prison and police managed to trace the drone to its operator.

Overview

A DJI Phantom 3 drone carrying marijuana, a mobile phone, phone chargers, headphones and several cigarette lighters got caught in a net above the fence perimeter of Central Mississippi Correctional Facility. Facility security guards retrieved the drone and passed it to the local investigators to attempt to track down the operators. Rankin County police investigators were able to obtain forensics from the drone's telemetry and flight data and traced the drone to an address in Vicksburg where it was used frequently. Security camera footage from the surrounding buildings helped to ascertain the culprits and both the drone operator and his accomplice were apprehended.

Analysis

This incident reflects the growing adaptation of utilising drones to carry out illicit operations. Individuals and criminal groups are realising that drones are an innovative solution against traditional methods of delivering contraband into restricted areas.

Drones are easily available off the shelves and are known to reduce risk to the operators from being spotted and apprehended by law enforcement agencies as operators are located away from the immediate area of crime. In addition, these small sized drones can carry loads of up 5kg and can hover in the air for a long time at a high altitude, giving it an advantage to stay hidden until it is time to drop the payload. Offenders for such deliveries tend to get away easily as many secured or restricted facilities do not yet possess drone detection or counter-drone systems to mitigate the growing threat of drone intrusion.

Delivering contraband items via a drone requires a bit of knowledge and skill; offenders must think of ways to be able to carry the items, travel amidst environmental conditions and release the items at the appropriate time. Failure to secure or release the items correctly will result in a failed delivery, or to an unintended recipient.

The risk of being traced due to visual sighting or forensics on a downed drone (via its video and photo footage) poses an exposure risk to the operators, which law enforcement officers can make use of, as reflected in this incident. Operators are not impervious from identification as the drone video footage and telemetry can allow law enforcement to trace the drone back to its take-off point. Facial recognition of the offenders may also be captured within the video, allowing easier investigation and apprehension of the offenders.

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 recommends for a drone threat management Standard Operating Procedure (SOP) or incident response plan be drafted to govern the process, people and methodology in handling a drone, collecting evidence and responding to potential drone incidents. Security agencies can undertake mock simulations and training scenarios in reacting to such rogue drone incidents to test and hone their response, improve communication flow between participating agencies, practice on the logging and monitoring of drone cases, mitigate risk and surface any challenges faced during the simulation.

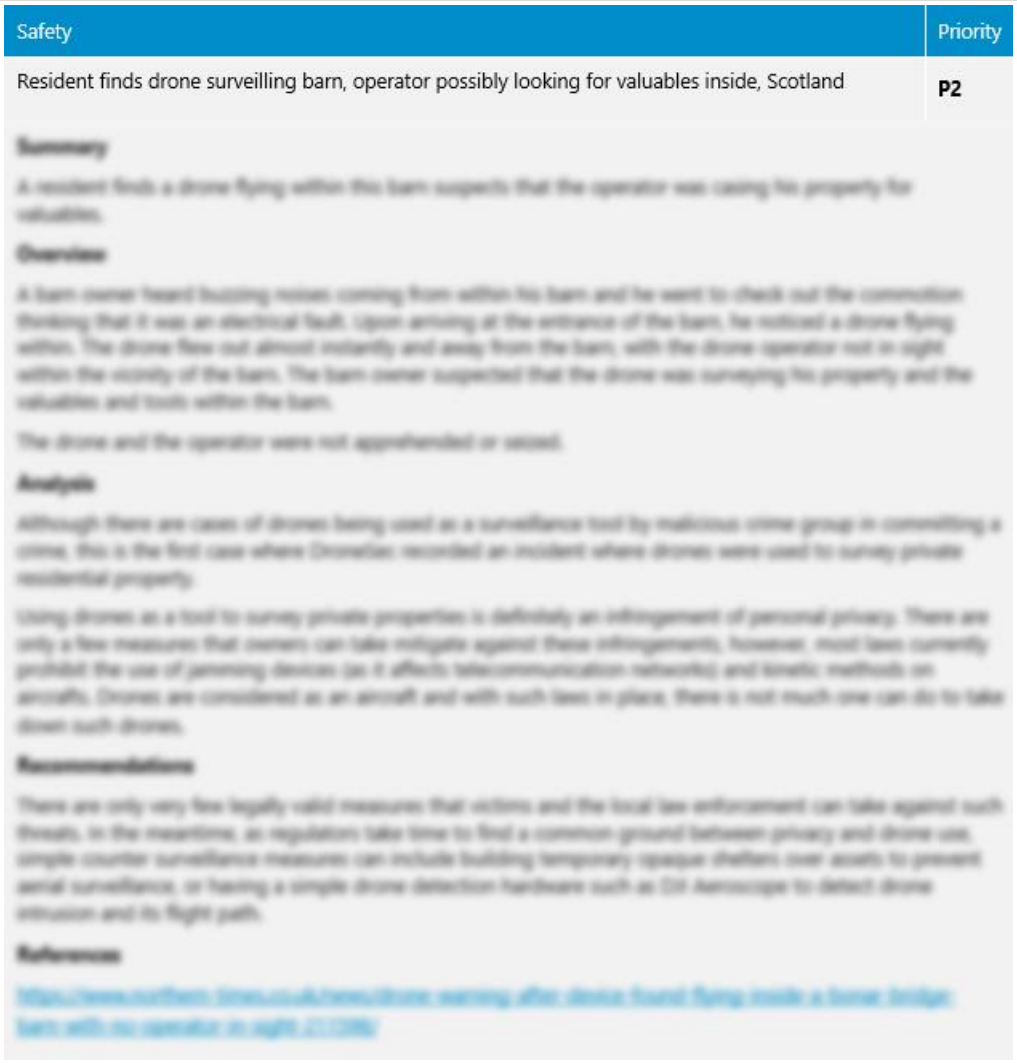
In cases like this incident where the drone has crashed, forensic analysis of the drone's telemetry would be incredibly useful. Event analysis from the drone data and video footage could assist in recognising take-off and landing zones and may aid in seizure or prevention of future attempts of drone incursions.

Finally, enforcement agencies should appeal to the help of the public as an eyewitness or via the use of existing CCTV installed in surrounding buildings. Such information is beneficial as such evidence can lead to the discovery and arrest of persistent rogue drone operators.

References

https://www.clarionledger.com/story/news/2020/09/09/2-men-facing-charges-after-drone-carrying-contraband-crashes-cmcf/5764303002/

https://www.wlbt.com/2020/09/09/arrested-after-drone-used-sneak-drugs-into-prison-mdoc-officials-say/



Safety	Priority
Resident finds drone surveilling barn, operator possibly looking for valuables inside, Scotland	**P2**

Summary

A resident finds a drone flying within his barn suspects that the operator was casing his property for valuables.

Overview

A barn owner heard buzzing noises coming from within his barn and he went to check out the commotion thinking that it was an electrical fault. Upon arriving at the entrance of the barn, he noticed a drone flying within. The drone flew out almost instantly and away from the barn, with the drone operator not in sight within the vicinity of the barn. The barn owner suspected that the drone was surveying his property and the valuables and tools within the barn.

The drone and the operator were not apprehended or seized.

Analysis

Although there are cases of drones being used as a surveillance tool by malicious crime group in committing a crime, this is the first case where DroneSec recorded an incident where drones were used to survey private residential property.

Using drones as a tool to survey private properties is definitely an infringement of personal privacy. There are only a few measures that owners can take mitigate against these infringements, however, most laws currently prohibit the use of jamming devices (as it affects telecommunication networks) and kinetic methods on aircrafts. Drones are considered as an aircraft and with such laws in place, there is not much one can do to take down such drones.

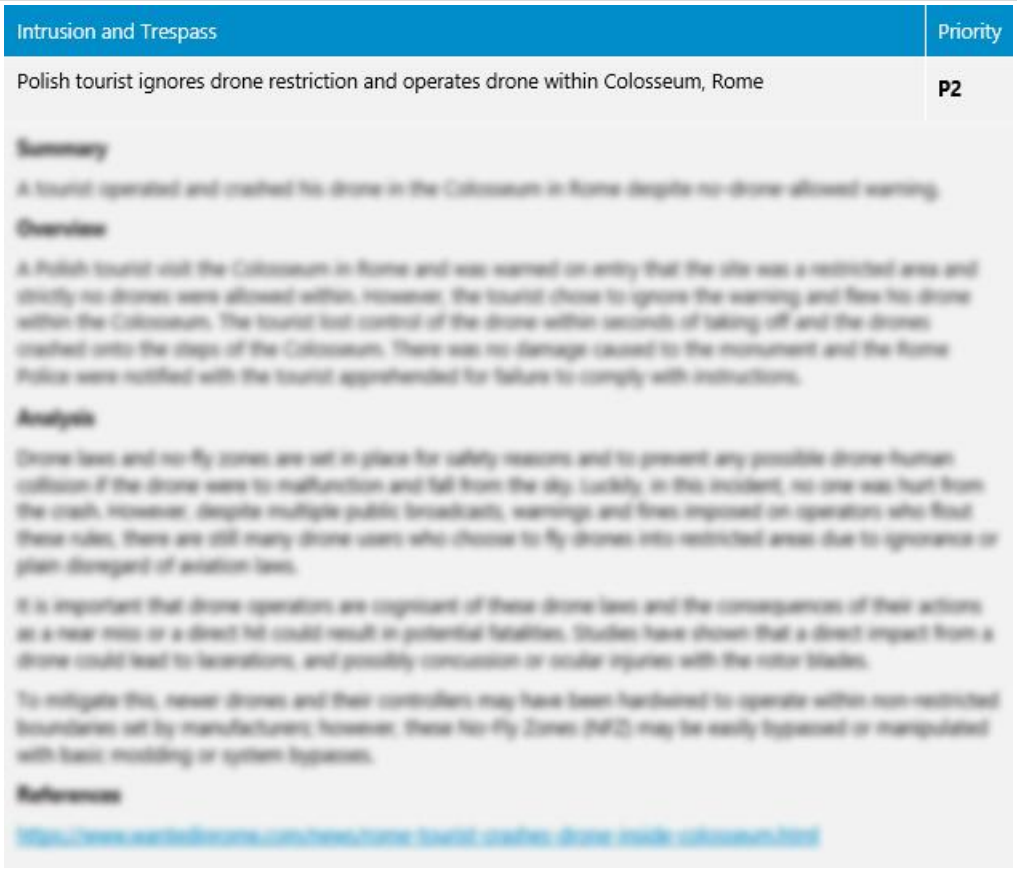
Recommendations

There are only very few legally valid measures that victims and the local law enforcement can take against such threats. In the meantime, as regulators take time to find a common ground between privacy and drone use, simple counter surveillance measures can include building temporary opaque shelters over assets to prevent aerial surveillance, or having a simple drone detection hardware such as DH Aeroscope to detect drone intrusion and its flight path.

References

https://www.northern-times.co.uk/news/drone-warning-after-device-found-flying-inside-a-bonar-bridge-barn-with-no-operator-in-sight-211096/

Figure 1 - Can't see this post? Get in touch with the DroneSec team to get access.



Intrusion and Trespass	Priority
Polish tourist ignores drone restriction and operates drone within Colosseum, Rome	P2

Figure 2 - Can't see this post? Get in touch with the DroneSec team to get access.

1.3. CYBER AND DATA SECURITY (P3)

Kittyhawk releases guidance on cyber-security elements for drone and UTM manufacturers

https://kittyhawk.io/wp-content/uploads/2020/09/Kittyhawk-Security-White-Paper.pdf

1.4. NEWS AND EVENTS (P3)

Lebanese Army shoots down intruding Israeli drone in Aita al-Shaab, Lebanon

https://www.timesofisrael.com/lebanese-army-claims-to-shoot-down-idf-drone-over-its-airspace/#gs.fux34c

Saudi-led coalition destroys two bomb-laden drones from Houthi terror group in Yemen

https://www.reuters.com/article/us-saudi-security-yemen/saudi-led-coalition-destroys-explosive-laden-drone-launched-by-houthis-idUSKBN2610B2

Pakistani Army shoots down intruding Indian quadcopter in Jammu and Kashmir

https://www.dawn.com/news/1578898/indian-spying-drone-shot-down

India shoots down Pakistani 17.5kg drone carrying 5.5kg payload of weapons and components

https://www.oneindia.com/india/alert-along-loc-after-isi-uses-drones-to-drop-weapons-for-terrorists-3146997.html

Indian Police suspect weapons seized in a highway were dropped from a cross-border drone

https://www.greaterkashmir.com/news/front-page-2/weapons-recovered-on-highway-were-dropped-by-drone-in-samba-dgp/

Operator apprehended due to drone flying within Elstree Aerodrome runway, London

https://www.watfordobserver.co.uk/news/18721122.drone-dangerously-flown-restricted-airspace/

Thousands of unauthorised drone flights detected in Berlin's government district

https://translate.google.com/translate?hl=en&sl=de&u=https://www.welt.de/politik/deutschland/article215434130/Drohnen-im-Regierungsviertel-Tausende-Fluege-ueber-Berlin.html&prev=search&pto=aue

Oakland County Airport officials announce near-miss incidents with drones and aircraft

https://www.fox2detroit.com/news/airplanes-helicopters-seeing-more-close-calls-with-surge-in-drone-use

Dog kidnappers use drones and social media to surveil victims before stealing dogs

https://www.newstalk.com/news/dog-nappers-using-drones-facebook-steal-peoples-pets-1073342

Helensburgh Police issues warning to residents on flying drones over populated areas

https://www.helensburghadvertiser.co.uk/news/18722941.police-issue-warning-drone-flying-helensburgh-area/

1.5. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P4)

Drone industry stakeholders urge US FAA to make essential changes to proposed remote ID rule

https://dronedj.com/2020/09/11/letter-to-faa-please-reconsider-your-remote-id-proposal/

CASA seeks feedback on proposed changes to rules on drone licensing and operations

https://consultation.casa.gov.au/regulatory-program/cd-2014us/consult_view/

Bangladesh releases new drone registration and guidelines for drones below 5kg

http://www.unb.com.bd/category/Bangladesh/no-permission-needed-to-fly-toy-drones-cabinet/57394

USA Department of Justice releases findings on Bureau of Prisons' capability to deter drones

https://oig.justice.gov/reports/audit-department-justices-efforts-protect-federal-bureau-prisons-facilities-against-threats

https://oig.justice.gov/sites/default/files/reports/20-104.pdf (PDF Document)

USA Department of Justice release report on efforts to protect BOP facilities against UAS threats

https://oig.justice.gov/news/doj-oig-releases-report-dojs-efforts-protect-bop-facilities-against-threats-posed-unmanned

https://oig.justice.gov/sites/default/files/2020-09/2020-09-15.pdf (PDF Document)

Mysterious drone incursions have occurred over U.S. THAAD anti-ballistic missile battery in Guam (commentary)

https://www.thedrive.com/the-war-zone/36085/troubling-drone-incursions-have-occurred-over-guams-thaad-anti-ballistic-missile-battery

UK Defence Secretary highlights necessity of drones in future warfare (commentary)

https://www.dailymail.co.uk/news/article-8731999/Defence-Secretary-Ben-Wallace-signals-drones-replace-soldiers-battles-future.html?ns_mchannel=rss&ns_campaign=1490&ito=1490

One company could transform U.S. drone industry (commentary)

https://www.forbes.com/sites/davidhambling/2020/09/10/one-company-could-transform-us-drone-industry/#50d7908f5261

Terrorist use of commercially available drones (commentary)

https://media-exp1.licdn.com/dms/document/C561FAQFU3gWO6CAhxw/feedshare-document-pdf-analyzed/0?e=1600358400&v=beta&t=QMEVzei-rDTolzxl5YRJlgwhAQvxecC9kbp9v96SIdI

1.6. COUNTER-DRONE SYSTEMS (P4)

U.S. FAA opens invite for airports to host counter drone research programme

https://www.unmannedairspace.info/counter-uas-systems-tenders/faa-seeks-four-airport-operators-to-participate-in-uas-detection-and-mitigation-research-programme/

Boeing's new CUAS system, Compact Laser Weapon System, successfully tested at Nevada

https://defence-blog.com/news/boeing-mobile-laser-gun-successfully-defended-a-convoy-against-drones.html

UK Ministry of Defence opens innovation call for solutions to complex urban drone operations

https://www.gov.uk/government/news/innovation-call-for-urban-drone-technology

Department 13 affiliates with AUVSI to showcase counter drone solutions and technology

https://department13.com/department-13s-advanced-drone-technology-takes-off-with-auvsi/

1.7. UTM SYSTEMS (P4)

Collins Aerospace, L3Harris Technologies and Thales USA to trial Volansi's VOLY C10 for state-wide BVLOS operations

https://dronelife.com/2020/09/11/north-dakota-is-building-a-statewide-bvlos-network-for-drones/

Elbit Systems completes flight demo with Hermes 900 for UK maritime and coastguard agency

https://elbitsystems.com/pr-new/elbit-systems-uk-demonstrates-hermes-900-maritime-search-rescue-flights-for-the-maritime-and-coastguard-agency/?pageid=PR%20-20%20News

NASA releases report on unmanned performance from UTM Technical Capability Level 4 demonstration

https://www.unmannedairspace.info/latest-news-and-information/nasa-releases-report-on-strategic-deconfliction-following-flight-tests-at-uas-test-sites/

1.8. INFORMATIONAL (P5)

US Navy to host "Drone Wars 2021", a military exercise for unmanned systems

https://interestingengineering.com/the-us-navy-will-hold-drone-wars-2021-battle-tests-in-pacific

US Army to hold an open RFI for its Future Tactical Unmanned Aerial System programme

https://www.janes.com/defence-news/news-detail/us-army-plans-full-and-open-competition-for-ftuas

Clarke County and Jackson PD searches for missing man with help of drone, United States

https://www.wkrg.com/news/law-enforcement-searches-with-drone-for-missing-man-in-clarke-county/

Manchester Police located hiding man with help of thermal sensor drone, United States

https://manchesterinklink.com/police-use-drone-to-find-man-hiding-on-hall-street-after-allegedly-stealing-gun-from-car/

Chinese Army in Tibet deploy drones for rapid logistic support

https://www.janes.com/defence-news/news-detail/pla-troops-in-tibet-deploying-uavs-for-logistics-support

South Korea invests 2.7 trillion Won to develop drones for military use

http://www.koreaherald.com/view.php?ud=20200915000169

CAL Fire reminds public against use of drones near wildfires

https://www.nifc.gov/drones/index.html

China successfully trial combat system for integrated drone swarm and armoured vehicles

https://www.armyrecognition.com/weapons_defence_industry_military_technology_uk/chinese_army_tests_drone_swarm_and_armored_vehicle_integration.html

1.9. DRONE TECHNOLOGY (P5)

Anduril launches Ghost 4 helicopter-like drone for military use with modular payload system

https://medium.com/anduril-blog/anduril-introduces-ghost-4-c12d8c783930

European GNSS pushes for integration of European navigation satellite with drone operations

https://www.suasnews.com/2020/09/egnss-at-the-core-of-the-drone-revolution/

AirMap and U.S. DoD partner to develop AirBoss intelligence platform for military drones

https://www.businesswire.com/news/home/20200909005245/en/AirMap-DoD-Partner-Develop-AirBoss-Aerial-Intelligence

Boeing Australia completes first engine run on Loyal Wingman drone for RAAF

https://theaviationist.com/2020/09/14/boeing-has-completed-engine-run-on-first-unmanned-loyal-wingman-aircraft-for-australia/

AlarisPro launches platform for fleet management and predictive analytics on drone maintenance

https://www.alarispro.com/2020/09/alarispro-provides-enterprise-uas-operators-and-fleet-managers-with-powerful-new-features-for-improved-decision-making/

Sky Drone trials 5G network for drone operations with Hong Kong telecom, China Mobile HK

https://dronelife.com/2020/09/14/sky-drone-flies-the-5g-sky-with-hong-kong-telecom/

40km drone delivery to be trialled between Cornwall and Isles of Scilly

https://www.inyourarea.co.uk/news/drones-to-be-trialled-between-cornwall-and-isles-of-scilly/

1.10. SOCIALS (P5)

Drone used to capture video of San Francisco orange skies due to wildfires

https://www.youtube.com/watch?v=dSreOPz0Zcs

https://www.youtube.com/watch?v=F-zrRwBxbaM

Blog post teaches how to deliver and drop items from DJI Mavic Air 2 drone

https://thmoore.blogspot.com/2020/09/how-to-deliver-beer-by-drone.html

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.

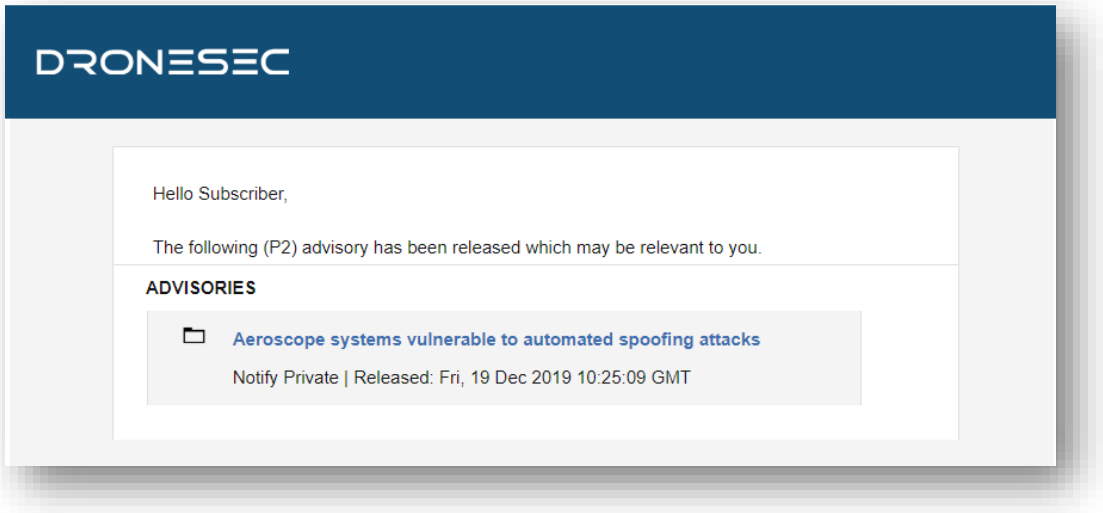


Figure 3 - A threat notification specific to a Notify customer's listed keywords.

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.