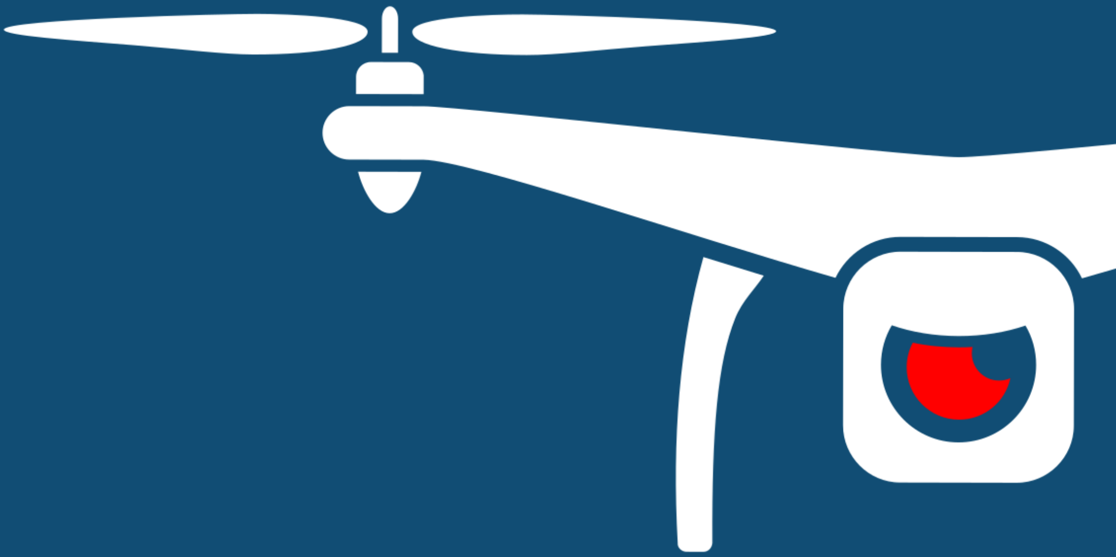
DRONE SEC

A Privasec COMPANY

NOTIFY ISSUE #39 (PUBLIC)

WEEKLY THREAT INTELLIGENCE

09 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

We're just over one week away from the Global Drone Security Network; live-streamed over 8 hours, over multiple countries and time-zones, we're certainly going to make recordings available where possible. Speaker schedules will be released this week, so thank you to everyone who signed up and will be participating as a speaker.

If you didn't know already, DroneSec specialises in hacking and security assurance services within drones. This extends to red teaming and threat simulations – something our team continually improves on through threat intelligence and modelling after adversary incidents. This newsletter is a small summary of public information that goes out on a weekly basis. If your organisation recognises the importance of real-time, on-demand technical analysis and dissemination of UAV threat intelligence, we have tailored offerings that can fill those gaps.

A number of featured incidents and whitepapers worth reading this week, and as always, these can be accessed in real-time via the Notify UAV Threat Intelligence Platform when they occur. Wishing everyone still in lockdown the best of health and an incident-free week.

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
Australian police appeal for information on failed drone delivery into Long Bay prison	**P2**

Summary

Police are looking for information after a drone carrying narcotics and contraband was found crashed near the Long Bay prison, Sydney Australia.

Overview

A member of the public found a crashed drone 300m away from Sydney's Long Bay Correctional Complex and reported the incident to the authorities. The drone was found carrying prescription drugs, buprenorphine, a SIM card and other electronic items.

Correctional officers mentioned that a fight occurred in the prison one day later due to drugs related matters and discovered that the prisoners was waiting for a drone to deliver drugs to the prison as supply within the prison ran short and visitors were banned from visiting the prison due to COVID-19.

It was unclear if the incident drone was meant for that purpose as investigation is still ongoing. The Australian law enforcement agency has released a CCTV video identifying two men, spotted in a DJI store recently, who might be related to the incident.

Analysis

This is the third case of drone deliveries into prisons in Australia during the past 2 months. Drones are easily available off the shelve for everyone; drones are known to reduce risk to the operators from being spotted and apprehended by law enforcement agencies as they are located some distance away from the immediate area of operation. 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.

This incident reflects the growing adaptation of Australians utilising drones to their advantage to carry out illicit operations. Organised crime groups and individuals are realising that drones are an innovative solution against traditional methods of delivering contraband across restricted areas. However, 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.

Threat Actor Profile
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
- DJI Mavic
- 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 continues to recommend the Australian government and law enforcement agencies be ready for a possible surge in unlawful use of drones in the near future as seen from cases globally. Basic drone mitigation and preparation measures are recommended to be set in place to respond to such incidents. Counter-drone systems that allow the detection of drones serve as a good step towards the prevention of drone deliveries. However, these systems are costly and partial purchases may not fulfill the criteria necessary for a full area protection.

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. Agencies should start taking notice of aerial infringements and adjust their patrol timings and routes as these schedules could have already been recorded and logged by the criminal gangs or groups. 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.

Finally, enforcement agencies should appeal to the help of the public as an eyewitness. Public community information is beneficial as such evidence can lead to the discovery and arrest of persistent rogue drone operators.

References

https://www.smh.com.au/national/nsw/appeal-for-information-after-drone-carrying-drugs-sim-card-found-near-long-bay-20200909-p55tq5.html

https://www.dailymail.co.uk/news/article-8711915/Drone-packed-drugs-near-notorious-maximum-security-jail.html

https://www.facebook.com/nswpoliceforce/posts/10158238308426185

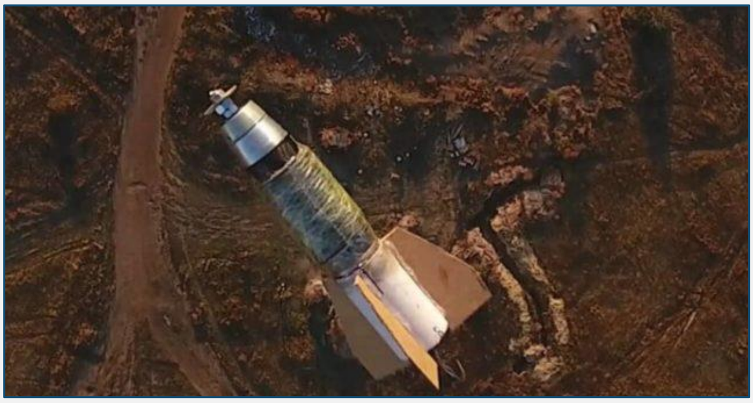
Safety	Priority
Pro-Russian separatists drop modified grenades onto Ukraine Armed Forces via drones	**P2**

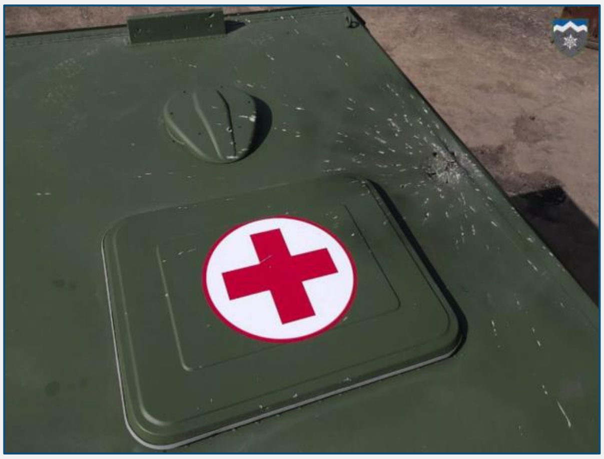
Summary

Despite a ceasefire agreement, pro-Russian separatists targeted Ukraine military troops using grenades dropped from a drone, injuring two servicemen.

Overview

The new ceasefire agreement between Ukraine and Russia-backed separatists in eastern Ukraine was formed in late July 2020 where the use of drones was clearly prohibited. However, Ukraine Armed Forces reported VOG fragmentation grenades (from grenade launchers) were dropped on several occasions, injuring patrolling soldiers. The drones were not sighted or seized but reports from the Ukraine Armed Forces have shown evidence of damages from such grenade bombs, causing structural damage to armoured vehicles.





Analysis

This is the second case DroneSec has recorded in the past 2 weeks of drone carrying explosive payloads to target personnel. The use of such explosive-laden drones have been recorded in the war against the Islamic State (IS/ISIS/ISIL), which has transitioned from battlefield tactics to use within urban and civilian environments via isolated 'lone wolf' attacks. The use of drone to deliver explosive payloads has been seen before in Guanajuato, Mexico and where drones were used to target rival gangs and state figures respectively.

With the rise in use cases of drones globally, more people, and malicious actors, are seeing the benefits of drones. This incident reflects the growing use of drones to carry out illicit operations and attacks. Organised crime groups and lone wolf terrorists are realising that drones are an innovative solution to complement traditional methods of war crimes. Drone attacks can easily drive fear among citizens and soldiers, allowing state actors to gain dominance of the locality.

Payload-capable drones are a cost-effective and risk-reduced technique which allows the drone operators to distance themselves from the immediate area of operations. Malicious users can operate safely with a low risk of being apprehended by law enforcement agencies and have sufficient time to escape once the operation has succeeded or failed. Offenders for such acts tend to get away easily as many common public areas do not possess drone detection or counter drone systems to mitigate the threat. Another advantage of using these small sized drones is its capability of hovering in air quietly for a long time at a high altitude, giving it an advantage to stay hidden until it the explosive ordinance is dropped. Operating the drone itself has a low skill barrier, however, in this situation, some operator experience and domain knowledge required in developing the release mechanism and remodelling of the drone.

Threat Actor Profile:

Motivation and Goals:

- To conduct ranged, loitering and weaponised attacks via drones with explosive payloads attached

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, urban and civilian environments
- Sourcing cheap and available Commercial-Off-The-Shelf drones for ranged attack strategies
- Sourcing cheap modifiable drones off the black market or second-hand market
- Extending the range and payload-carrying capacity of COTS drones for malicious missions by modding
- Training war fighters and soldiers in unmanned and counter-drone UAS flights and operations
- Using small COTS drones to drop explosive payloads (mortars, grenades ~<1 kg) on military units, often with shuttlecocks, PVC or home-made flight guidance mechanisms
- Using custom and purchased amplifiers, transmitters, receivers, antennas, extenders and dual-battery components to improve the overall range and targeting of limitations by OEM systems

Recorded Use of Drone/Equipment:

- Quadcopters, Multi-rotors, VTOL UAV, Fixed-Wing

Recorded Contraband/Crime:

- Drones attached with explosives/modified grenade

Recommendations

DroneSec recommends the military, authorities and law enforcement agencies to be prepared and ready for such threats and to have basic preparation measures set in place to respond to such incidents. Such aerial threats may be hard to detect and while it may not be possible yet to provide wide area coverage of drone detection and counter-drone systems, basic preparation measure can be set in place to respond to such incidents. A drone threat management plan and Standard Operating Procedure (SOP) should be drafted to govern the process, people and methodology in handling a drone threat.

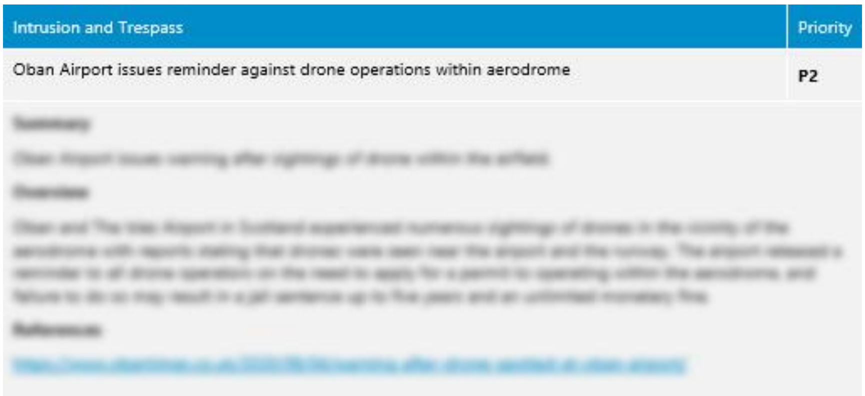
For battlefield operators, a number of deceptive or camouflage techniques are available to reduce the probability of being sighted by adversary UAS. Mobile and fixed drone detection and mitigation systems can aid in providing early-warning response times. For troops, enemy UAS should be treated with the same caution as IED's, but in a mobile and air-borne context. Small-arms fire may not be adequate to combat UAS, and the location of troop positions should be considered as compromised if spotted. Whilst most adversary drones have their LED lights taped over or removed, troops should be cognisant of small lights visible at night which could indicate adversary UAS in the area.

References

https://informnapalm.org/en/militants-drops-vog-grenades-from-drones/

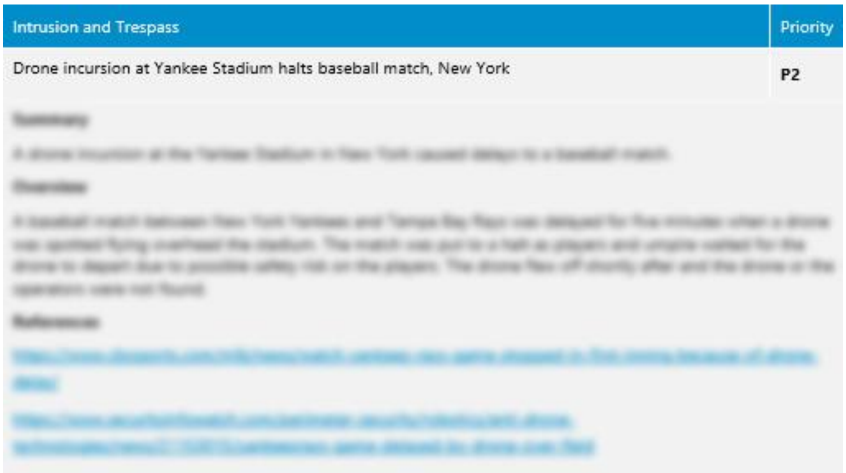
Intrusion and Trespass	Priority
Packets of narcotics dispersed over Tel Aviv via drone drop, Israel	P2

Figure 1 - Can't see this article? Get in touch with the team to chat about Notify Private: info@dronesec.com



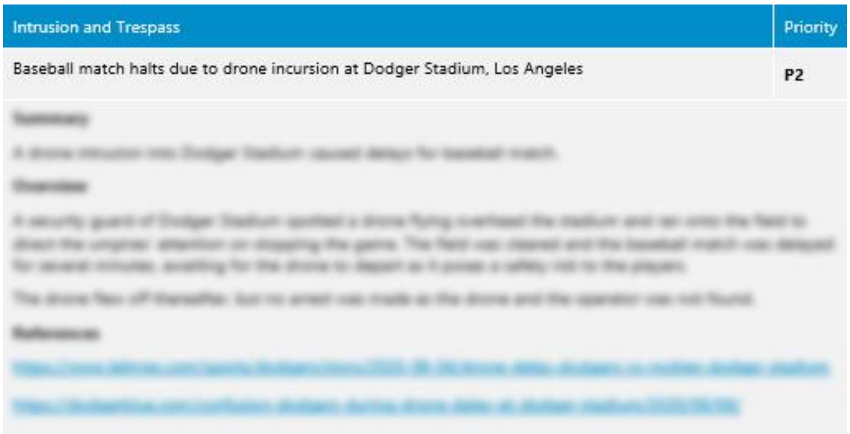
Intrusion and Trespass	Priority
Oban Airport issues reminder against drone operations within aerodrome	**P2**
[illegible]	

Figure 2 Can't see this article? Get in touch with the team to chat about Notify Private: info@dronesec.com



Intrusion and Trespass	Priority
Drone incursion at Yankee Stadium halts baseball match, New York	**P2**
[illegible]	

Figure 3 Can't see this article? Get in touch with the team to chat about Notify Private: info@dronesec.com



Intrusion and Trespass	Priority
Baseball match halts due to drone incursion at Dodger Stadium, Los Angeles	**P2**
[illegible]	

Figure 4 Can't see this article? Get in touch with the team to chat about Notify Private: info@dronesec.com

Safety	Priority
Drone operator halts descend of drone to avoid near miss with incoming passenger airplane	**P2**

Summary

A drone operator with legal permit spotted a passenger plane on approach and immediately halted the descend of his drone to avoid a possible mid-air collision.

Overview

Four two-passenger Cessna planes were flying in the Gamston Airport aerodrome, together with a permission-approved emergency services drone operator flying his drone within the airport's 5km radius. During the drone's descent from 400ft (121m), the operator noticed one of the Cessna planes flying towards him at 200ft (60m), between himself and the drone. The operator immediately halted the descent and allowed the plane to fly right in between before he continuing with the descent.

Findings from the UK Airprox Board showed that the Cessna pilots were told of the drone's activities but the pilot may have mistaken the drone's location, performing a short descent flight path, resulting in flying between the drone operator and the drone. Although members of the UK Airprox Board deemed the incident to have no risk of collision as the drone operator had full knowledge of the plane's movement, it was of both pilot's and operator's responsibility to avoid such possible mid-air collision.

Analysis

This incident is a positive reflection on aviation awareness that drone operators should aim to inculcate and possess, which is a fundamental aviation lesson that is taught to all manned aircraft pilots. Aviation awareness will allow drone operators to take note of his surroundings while carrying out drone operations, taking into account other aircrafts in the vicinity and released Notices to Airmen (NOTAMs). This forms a basic safety precaution for manned and unmanned operations within the same aerodrome.

However, as drones can operate beyond the operator's line-of-sight, drone operators may be required to adopt other measures to ensure unnecessary risk is not imposed on existing aircrafts, and safety is upheld in the aviation industry. As such, federal aviation authorities have been trying to come up with beyond line of sight procedures for such operations, but with a slow progress. Despite that, drone operators must be cognisant of the existing drone laws set in place by their country and adhere to them as these laws are set to prevent any possible drone-human and drone-aircraft collisions.

Recommendations

It is the responsibility of drone operators too, not just manned aircraft pilots, to ensure flight safety. Hence, DroneSec recommends for all aviation training schools and federal/state aviation agencies to consider providing fundamental aviation lessons, which are taught to manned pilots, to all drone operators when they are registering their drones. Such training will inculcate the habit of flight safety for drone operators, such as checking for Notice to Airmen (NOTAM) before any drone operations, and being ready to handle emergency situations in the event of a malfunction.

Ultimately, drone operators should have a good understanding on the capabilities of their drones – flight time, range and protocols or frequencies in use. These are important details leading to safe flights, aiding operators in planning their pre-flight mission and handling ad-hoc changes when unexpected events or contingencies occur mid-flight.

References

https://www.worksopguardian.co.uk/news/drone-and-two-seater-plane-near-miss-near-gamston-airport-2960771

1.3. CYBER AND DATA SECURITY

DJI to expand local data mode privacy protections to all models and mobile applications

https://www.suasnews.com/2020/09/dji-expands-data-privacy-protections-for-government-and-commercial-drone-operators/

1.4. NEWS AND EVENTS (P3)

Dozens more mystery drone incursions over U.S. nuclear power plants revealed (commentary)

https://www.forbes.com/sites/davidhambling/2020/09/07/dozens-more-drone-incursions-over-us-nuclear-power-plants-revealed/#5adba8b36296

Five men fined, drone seized for flying drone illegally over national reserve forest, India

https://timesofindia.indiatimes.com/city/coimbatore/chennai-men-fined-for-using-drone-cam-in-tiger-reserve/articleshow/77967824.cms

Man from County Tyrone charged for harassment and stalking, Northern Ireland

https://www.belfasttelegraph.co.uk/news/northern-ireland/man-faces-multiple-charges-over-flying-drone-39512134.html

1.5. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P4)

Thailand CAA appoints UK CAA to draft drone regulations for integration into existing legislation

https://www.suasnews.com/2020/09/uk-caai-to-draft-drone-regulations-for-thailand/

Oman releases laws on the registration and operation of drones

https://timesofoman.com/article/3018892/oman/oman-puts-in-place-new-law-regulating-drone-usage

Terror and technology from dynamite to drones (commentary)

https://warontherocks.com/2020/09/terror-and-technology-from-dynamite-to-drones/

Teardown of DJI drone reveals 80% parts are COTS, many from the US (commentary)

https://asia.nikkei.com/Business/China-tech/Teardown-of-DJI-drone-reveals-secrets-of-its-competitive-pricing

Trump ban on Chinese drone parts risks worsening wildfires (commentary)

https://arstechnica.com/tech-policy/2020/09/trump-ban-on-chinese-drone-parts-risks-worsening-wildfires/

Advancing drone technology innovation in government (commentary)

https://fedtechmagazine.com/article/2020/09/advancing-drone-technology-innovation-government

Protecting Against Rogue Drones – Congressional Research Service

https://fas.org/sgp/crs/homesec/IF11550.pdf (PDF Document)

Three Considerations Around Drone Noise and Strategies for Mitigation (whitepaper)

(PDF available in the Notify Platform)

1.6. COUNTER-DRONE SYSTEMS (P4)

General Dynamics Mission Systems to sell Dedrone CUAS detection and defeat system

https://www.dedrone.com/press/dedrone-and-general-dynamics-mission-systems-enter-partnership

NATO develops in-house CUAS technology for use across member nations

https://www.unmannedairspace.info/counter-uas-systems-and-policies/nato-develops-in-house-counter-uas-technology-for-dissemination-across-member-nations/

U.S. military, Israel DoD collaborate with XTEND for Sparrowhawk AR counter drone system

https://www.defensenews.com/unmanned/2020/09/08/israeli-startups-counter-drone-augmented-reality-system-to-deploy-with-us-forces/

Leonardo achieves IOC for ORCUS, modular and scalable CUAS system for Royal Air Force

https://des.mod.uk/counter-drone-programme-milestone/

1.7. UTM SYSTEMS (P4)

Yuneec and Droniq collaborate to fit H520 drones with HOD4track module for BVLOS operations

https://www.unmannedairspace.info/latest-news-and-information/droniq-yuneec-cooperation-offers-standard-tracking-solution/

Kittyhawk launches new LAANC capabilities for UTM systems

https://kittyhawk.io/blog/kittyhawk-launches-the-next-generation-of-laanc-utm/

Israel grants BVLOS permission to Percepto's drone in a box solution for Dead Sea operations

https://www.commercialdroneprofessional.com/percepto-gets-bvlos-permission-for-autonomous-drone-flight-in-israel/

FAA to begin second phase of UTM testing at Griffiss International Airport in Rome, New York

https://www.urbanairmobilitynews.com/utm/rome-usa-second-phase-of-federal-program-to-develop-high-density-air-traffic-control-for-drones-begins/

Telegrid Technologies successfully tests BVLOS drone delivery at Springfield Beckley Airport

https://www.springfieldnewssun.com/news/drone-express-takes-to-the-skies-above-springfield/SFXL2IKDRZAF3PNGR2QTLXSMQI/

1.8. INFORMATIONAL (P4)

Nigeria forms 203 Combat Reconnaissance Group for drone development and operation

https://www.blueprint.ng/war-against-terror-air-force-establishes-drone-base/

UK CAA to trial jamming activities on several frequencies: Luce Bay, Salisbury Plain, New Forest

https://skywise.caa.co.uk/jamming-trial-8-sep-4-dec-luce-bay/

https://skywise.caa.co.uk/jamming-trial-7-18-sep-salisbury-plain-and-new-forest/

US DoD launch pilot program testing potential employment of Skylord drones to the US military

https://m-jpost-com.cdn.ampproject.org/c/s/m.jpost.com/jpost-tech/us-military-to-employ-next-generation-israeli-drone-technology-641497/amp

South Africa firm Sentech looks to use fleet of drones for state and border security and law enforcement

https://www.businessinsider.co.za/sentech-wants-to-buy-autonomous-uavs-for-border-patrols-2020-8

1.9. DRONE TECHNOLOGY (P5)

SPH Engineering and Mondot offers real-time video management software for drones to Latvia

https://sph-engineering.com/news/a-drone-based-solution-to-increase-effectiveness-of-customs-control-of-the-state-revenue-service-of-latvia

LMT conducts cross border drone flight from Latvia to Estonia via mobile network

https://www.suasnews.com/2020/09/lmt-successfully-conducts-their-first-cross-border-drone-flight-on-the-mobile-network/

Brazil approves BVLOS delivery for Speedbird Aero with ParaZero parachute recovery system

https://parazero.com/2020/08/31/speedbird-aero-secures-historic-drone-delivery-authorization-in-brazil-using-parazero-safety-system/

IAI introduce drone helicopters for commercial uses, based off Alpha Unmanned Systems SUAS

https://www.iai.co.il/iai-introduces-multiflyer

US DIU selects Parrot as drone supplier for United States Government

https://blog.parrot.com/2020/08/31/parrot-diu-blue-suas/

DJI Matrice 600 drones preferred over helicopter for wildfire containment

https://coloradosun.com/2020/08/28/drones-dropping-dragon-eggs-colorado-firefighting-grizzly-creek/

Drone testing facility opens at Goodwood Aerodrome in Chichester, United Kingdom

https://www.aerospacetestinginternational.com/news/drones-air-taxis/drone-flight-testing-site-opens-in-the-uk.html

1.10. SOCIALS (P5)

Pennsylvania Public and Private UAS Symposium – UAS Mitigation Panel (webinar)

https://www.aerodefense.tech/pennsylvanias-public-and-private-uas-symposium

INTERPOL seeking partners in UAV threats, countermeasures based in SEAPAC for network

https://www.linkedin.com/posts/christopher-church-aa7aa144_drones-seasia-activity-6709282772156063744-bcBj

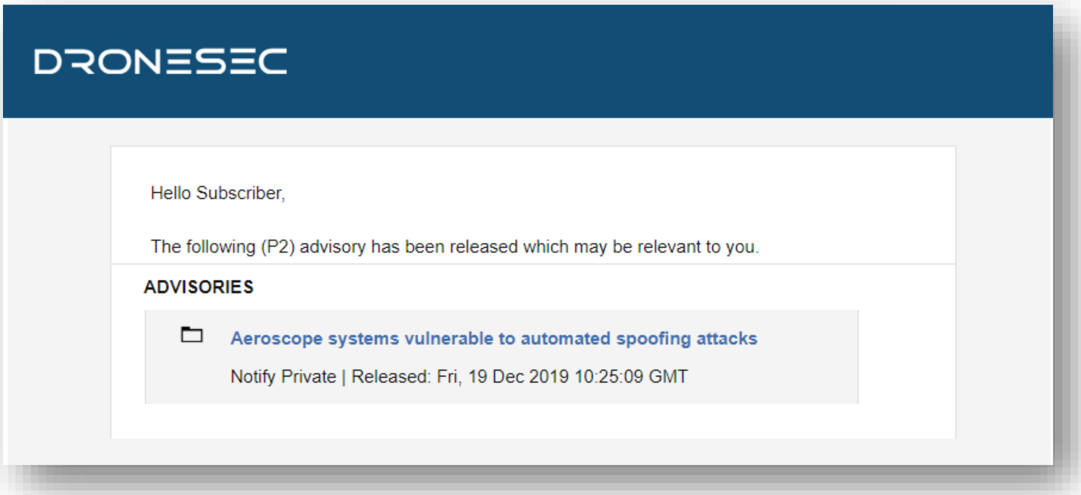
APPENDIX A: THREAT NOTIFICATION MATRIX

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.


DRONESEC

Hello Subscriber,

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

ADVISORIES

Aeroscope systems vulnerable to automated spoofing attacks

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

Figure 5 - 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.