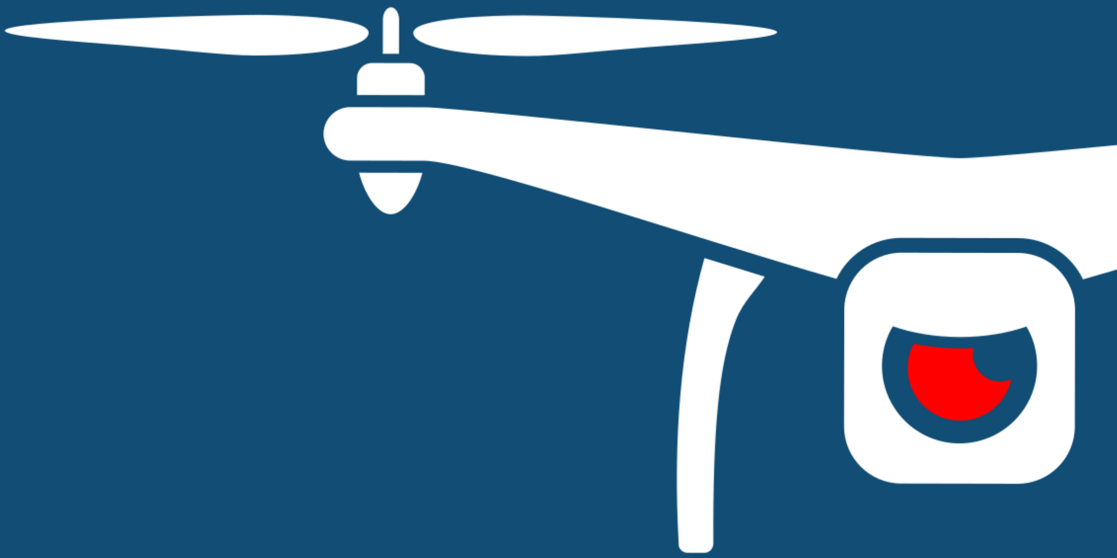
DRONE SEC
A Privasec COMPANY

NOTIFY ISSUE #27 (SPECIAL)

WEEKLY THREAT INTELLIGENCE

17 June 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 are pleased to announce the DroneSec Notify Threat Intel Platform will release tomorrow.

View the launch page by clicking here.

Officially of course – we'd like to both extend a heartfelt 'thank you' to those receiving our weekly threat intel reports, and those who have stuck with us for some time. Before we go public at 12pm AEST 18/06/2020, please take the opportunity to find out more about the platform.

The platform development has been a long time coming and is best summarised by a reflection from our Threat Intel lead, Arison Neo. I'll let him have the floor soon but first – we're releasing three paid tiers of subscription. Following the launch (and ironing out any surprises!) we'll be **opening up free registration tier access** to the platform on July 2nd (02/07/2020). It's really important we service our current paying customers first, so a staggered approach will give us time to support them with onboarding.

It's a huge moment for us. I'm proud of our team and the unique character they bring to each aspect of our operations. I'm also thankful to our customers – we have a very unique range of individuals and organisations that always provide us with new opportunities and approaches to reducing the risk of rogue UAS. Given the interest from educational and law enforcement agencies, we have preferential pricing if you fit into that category.

In addition to what's currently available, we have incredible line-up of features, additions and projects being released within the platform in the coming months. We'll be announcing these partnerships soon, with a focus on providing real-time, actionable threat intelligence, benchmarking UAS threat actors and providing global visibility to CUAS operations.

What happens to this newsletter?

Your Notify weekly reports will continue as usual. Changes will see (1) Featured Advisories and (2) Monthly Roll-Up details gradually moving to paid users within the platform. This is important to maintain quality and increase the analytical effort involved.

How can I view the platform if it only releases on July 2nd?

Current and new paid users will automatically be onboarded onto the platform.

For free users, we're more than happy to take you through a demo of the platform and its features. Simply visit the landing page, send us an email (info@dronesec.com) or approach us on slack.

-

It's important to recognise that this has never been done before – there is no benchmark or historical barrier of entry for Threat Intelligence collection of UAS/UAV/RPAS/Drones. We hope this platform, our intelligence collection methodologies and obsession-based staff will continue to increase security operations and reduce the risk of restrictions on this innovative, emerging technology industry. Please enjoy the below reflections looking back at our journey from internal tool to global drone threat intelligence and monitoring platform.

- *Mike Monnik, DroneSec CTO*

THE NOTIFY **JOURNEY**

Why we created a Threat Intelligence Platform for drones

Arison Neo – Drone Security Consultant (Threat Intelligence Lead) @ DroneSec

The problem

Over the years, drones have become a cornerstone of emerging technology in today's society. Drones speed up industrial processes and reduce the need for human contact in dangerous jobs, freeing up resources and time. However, it is not just the 'good guys' who are utilising drones but the 'bad guys' too. Drones, when employed safely, can be a mode of delivery across vast distances, conduct inspections in hazardous areas, or provide 3D modelling and surveys of large plots of land within minutes.

Similarly, drones can also be used to deliver contraband into restricted areas, conduct weaponised aerial strikes with payloads fitted onto a modified chassis, or be used for surveillance against physical targets. Incidents like the latter are not uncommon and local law enforcement agencies are increasingly apprehending drone-enabled offenders. Government, aviation authorities and militaries across the world have raised concerns about the possible and rising threat of drones and are taking measures to ensure the ease and cost of such threats do not enable an influx in drone-responsible incidents.

The information gaps

To better understand the threat vectors, red teaming is an essential activity within the drone sphere; that is, conducting a physical and digital security assessment against a perimeter, using the equipment often recorded as used by the malicious pilots.

The missing piece, however, is the Threat Intelligence (threat intel) that forms the substance of red teaming operations. These activities need to be intelligence driven; not just using the same equipment from real-life scenarios, but the tactics, techniques and procedures used by the threat actors themselves. As a result, threat intel becomes a history-books lesson; record everything, catalogue and use that information to better inform your active red team.

Notify was DroneSec’s attempt at sourcing better threat intelligence to uplift our red team operations; we didn’t want to use a COTS drone where the majority of threat actors in the region had historically used custom drones, or take off from a prison parking lot when most actors had historically sought out nearby forests as launch-zones. To define, threat intelligence is the gathering and understanding of threats and threat actors towards the aim of mitigating such threats through an informed decision, and red teaming is fundamentally about putting oneself in the minds of attackers and carrying out various conventional and unconventional ways and methodologies in taking down a specified target.

How we started

DroneSec gathers and triages drone incidents, placing the data in a repository where information can be filtered and sorted. In short, a knowledge base on the locations, time details, incident summaries, and make/models of drone(s) used. This forms the basis of the planning and collection phases of the threat intelligence cycle. At this stage, threat intelligence organisations will start to see the raw data, or a broad overview, on the kind of drone incidents that are occurring worldwide. This provides law enforcement agencies with generalised attack vectors, common equipment types and commonly targeted locations. The intelligence cycle for most threat intel organisations stop here as the requirement to process these huge amounts of raw data is labour intensive and resource demanding.

What we did

DroneSec by nature is a data-driven intelligence firm; even so, the information we were gathering was not enough to provide substantial use cases for our aerial threat and red team simulations. For some time, we gathered and processed global incidents on the drone ecosystem – only limiting ourselves to the three pillars of drone security: drones, counter-drones and UAS Traffic Systems (UTM). We built a substantial knowledge base of drone incidents while working with law enforcement agencies, drone organisations and cyber security researchers. We hired military drone pilots and military intelligence personnel to turn the raw data into meaningful information for understanding threats of drones of all shapes and sizes.

Our core team soon realised the complete gap in commercial threat intel for drones and the ineffectiveness (and signal to noise ratio) of utilising traditional cyber-security threat intel platforms for this need. We saw gaps in the drone ecosystem which were not addressed in today's society and that formed the initial basis of having a drone-centric newsletter.

One key driver for us as a firm, from the very start, was placing Actionable Threat Intelligence (ATI) at the core focus; we wanted to track and characterise the threat actors to the minute detail. Actionable Threat Intelligence (ATI) is the information given to decision makers allowing them to act upon, with an informed mindset, towards the formulation of a strategic, operational or tactical plan. ATI has allowed DroneSec to work towards a goal in mind, it has crafted the way we plan, direct, collect and process our threat intelligence methodology. This gave us the push to release a weekly threat intelligence newsletter, DroneSec Notify, as a way of continually tracking threat actors progress, innovation and tactical utilisation of new technologies and products. For each incident, our threat intel process is simple; log, tag, catalogue and analyse.

Some really interesting Threat Intel we've been able to grasp from recording these on a weekly basis includes:

- How long threat actors use a new drone system from its release date to use in a crime;
- The make/model of drones most commonly used for airports vs prisons vs stadiums;
- The cost, availability and use of payload dropping mechanisms in 'narcodrones';
- The Standard Operating Procedures (SOPs) used by law enforcement vs private organisations;

How we've done it

With ATI, our core focus shifted to expanding the intelligence we possessed - to ensure that our intelligence was not just a means to uplifting our red teaming, but providing data for early warning, pattern analysis and trend recognition for the 'blue teams' at the helm of counter-drone systems. With the proliferation of the Notify Drone Threat Intel weekly newsletter, our audience became crystal clear;

there are market segments that care about drone security far beyond law enforcement, counter-drone organisations and lawmakers. By learning what counter-drone 'blue teams' (that is, the defensive side) need to reduce their risk appetite and security posture, we were able to create some specific tools to aid their roles.

When we reached our limit of trying to do this through spreadsheets, we knew it was time to build a platform that could handle this. This led to the creation of Notify – as a platform. Completely designed and developed from the ground up, we set about thinking what type of information and markers would be needed to better enable our red team. How will drone information be displayed? Prioritised? What level of automation and how much human interaction on event triage? If we were a counter-drone operator, a security guard, an Air Traffic Control (ATC) tower or a government audit body; how could we display this information in a real-time and meaningful way? Long story short, the development of Notify has been one of change and adaption; its next few years of development will be incredibly interesting!

Interesting use cases along the way

DroneSec Notify helps law enforcement agencies. Analysis from Notify helped identify several heat zones in areas where drone incidents frequently occur. Not all of this information is gained at once – sometimes several sources are required to inform the full picture – for example, the 'peak hour' whereby offenders usually operate at, the typical ingress and egress path, the model of drones which are frequently used. Alone, somewhat helpful, in combination with several tracked conversations and videos observed online, very useful. This type of information provides a collection of insights in determining the modus operandi of malicious drone operators which have statistically led to the continued prevention of contraband delivery.

The second key use case is our ability to slot an act or incident into a 'category'. No more going blind with a drone 'incident'; it falls into a specific category, incident type and attack vector that we have previously measured and analysed. The best part about templating incidents like this is looking at the Root Cause Analysis (RCA) – similar incidents with different details may share the same characteristic or even threat actor, this makes defensive mitigation (or remediation steps) much easier to assess. Users of our ATI benefit from this – for example, by hammering home the same recommendation strategy for a 'class' of attack, a client recognised the possibility of a drone incident they had been exposed to (through Notify) and could make a time-crucial decision call as an early pre-empt. By analysing threat intel, organisations can also identify gaps without having to experience them first-hand and implement recommendations before actually facing the challenges themselves. How do you look through the eyes of someone who's experienced an incident first-hand? This is where Notify threat intel comes in – sources include first responders, organisations facing several drones threats a month or experienced implementors in the counter-drone space. Record, inform, uplift, repeat.

Reflections

DroneSec Notify has come a long way – from a small and humble beginning (uplifting our own internal practice) to working with interesting entities around the world on their complex (and often never-seen-before) drone security incidents. Our team's constant mission to improve and grasp this new technology will continue to form the foundation of our technology for many years; personally, I'll strive to bring you the most actionable and up-to-date threat intelligence in the drone ecosystem.

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.

These public reports are now available in a digital format, searchable database and live map system within the DroneSec Notify Platform.

Something we missed? Keen to become an intel 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 (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.

Notice to our readers: our featured advisories will slowly cease to be publicly available as DroneSec Notify moves to the online platform. Featured advisories have provided context and field-based learnings to important issues. However, with the ever-growing database that we have, DroneSec has moved onto an online repository where artefacts and reports can be tracked, classified and analysed much easier. Featured Analysis from now on are more comprehensive, wider in spectrum but only available on the Notify platform.

We thank you for your continued support thus far and we do look forward to having you together on our online Notify platform. Featured Advisories (only) will cease at beginning of July 2020; however, the free unclassified restricted PDF newsletter will still be available.

Security	Priority
Four arrested for failed attempt of drone delivery into Collins Bay Institution	**P2**

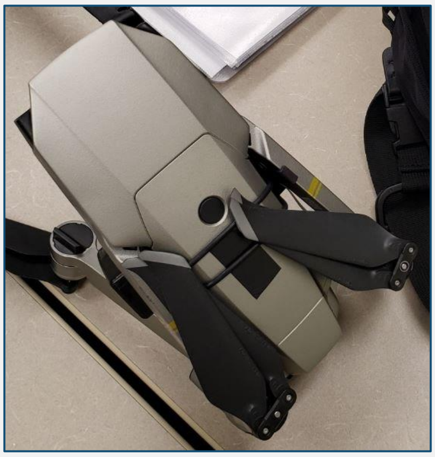
Summary

After months of investigation, four people in connection to a failed drone delivery to Collins Bay Institution was caught.

Overview

Correction officers of the Collins Bay Institution spotted a DJI Mavic drone flying in the vicinity of the prison on March 24th, 2020, at 4:00am in the morning. They traced the drone to a vehicle parked nearby containing two people. Upon searching the vehicle, they seized a drone, cannabis and cigars and apprehended the two suspects. Additionally, a package was also found within the prison grounds containing weapons, tobacco and cannabis.

After months of investigation, law enforcement officers were able to trace two additional suspects who were involved in the participation of the drone delivery. All four were charged with participation and conspiracy in committing an indictable offence.



Analysis

Tracked Actor Category:

Prison Drone Delivery (Local 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*
- *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*
- *In rare cases, utilising counter-forensics techniques by removing SD cards, disabling caching, destroying serial info and disabling the Return-to-Home functionality*

Recorded use of drone and equipment types:

- *Quadcopters, Multi-rotors*
- *PGYTECH Air Dropping System*

Using drones is a cost-effective technique with reduced risk on being spotted as operators are situation a distance away from the immediate area of operations. This allows malicious users to operate safely with a low risk of being apprehended by law enforcement agencies. In addition, these small sized drones can hover in air for a long time at a high altitude, giving it an advantage to stay hidden until it is time to drop the contraband. Offenders for such acts tend to get away easily as many facilities do not yet possess drone detection or counter-drone systems to mitigate the threat

We are starting to see more drone deliveries across prisons by organised groups as they realise that this is an innovative solution to delivery traditional methods of throwing packages across the walls. The low price point and availability of COTS drones still make drones an easily accessible tool. However, the risk of being traced due to visual sighting or forensics on a downed drone (via its video and photo footages) poses an exposure risk to the operators.

Recommendation

Collins Bay Institution is a hotspot for contraband deliveries. In the past, correctional officers have caught multiple offenders attempting to throw packages of contraband across the walls. Today, technology have enabled offenders to use drones for their illicit acts. Collins Bay have experienced at least three narcodrone incidents in the last year.

DroneSec recommends all local law enforcement agencies to be prepared and ready for such up and coming threats. While some facilities may have constraints in deploying counter drone solutions, basic preparation measure can be set in place to respond to such incidents. For example, 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.

Organisations should also aim to undertake mock simulations in reacting to such rogue drone incidents to test and hone their response, improve communication flow between agencies and practice on the logging and monitoring of cases. These simulations can aid law enforcement agencies in timing their response, mitigate risk and surface any challenges during the process.

References

https://nationalpost.com/pmn/news-pmn/canada-news-pmn/four-charged-after-investigation-into-drone-used-in-prison-smuggling

After July 2nd, 2020, featured advisories will be available to paid subscribers only. Contact info@dronesec.com to arrange a demo or visit https://dronesec.com/pages/notify to learn more.

Intrusion and Trespass	Priority
Chinese man arrested for crashing drone into elementary school	**P2**

Summary

A 49-year-old Chinese national was arrested in Japan for illegally flying this drone over an elementary school.

Overview

After locating a crashed DJI Mavic 2 drone in an elementary school in Tokyo, Toshima ward, in May 2019, the Tokyo Metropolitan PD issued a request for appearance for the owner of the drone. However, no one came forward for the drone. After a thorough investigation the PD found that the drone belonged to a 49-year-old Chinese national who lived within the same ward. The Chinese national was arrested for flying his drone without a proper permit, trespassing into prohibited airspace over an elementary school and operating the drone over a populated area. The crashed DJI Mavic 2 drone did not cause any bodily harm during the crash.

ドローン
小学校に落下 児童にけがなし
無許可で飛ばしたか 男を逮捕
東京 豊島区
豊島区上空における航空法違
押収されたドローン
~ドローン無許可·無承認飛行~
池袋警察署
池袋警察署

Analysis

This incident clearly reflects the environment and behaviourism of errant drone operators commonly observed in dense-populated areas - 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. Although errant drone operators are disconnected from the drone by distance and wireless transmissions, the risk of being traced due to forensics on video and photo footage may eventually lead to apprehended, if the drone system has been seized.

Recommendation

It is important that drone operators are cognisant of their local aviation laws or the consequences of their actions in a near miss or a direct hit could result in potential fatalities. Drone laws and no fly zones are set in place for safety and security reasons, but will only serve to restrict the drone industry and community further if operators continue to be ignorant with it.

While it may not be possible yet to provide city-wide coverage of drone detection and counter-drone systems, basic preparation measure can be set in place to respond to such incidents. A drone management plan and Standard Operating Procedure (SOP) should be drafted to govern the methodology in handling rogue drones. Enforcement agencies can also appeal to the help of the public as an eyewitness; it is beneficial to have a process for such evidence, and then carefully curated for collection and logging. Additionally, mock simulations can be conducted to hone response in time critical situations, improve communication flow between involved agencies and mitigate inherent risks and surface challenges in communication and regulatory requirements.

References:

https://www3.nhk.or.jp/shutoken-news/20200610/1000050020.html

After July 2nd, 2020, featured advisories will be available to paid subscribers only. Contact info@dronesec.com to arrange a demo or visit https://dronesec.com/pages/notify to learn more.

Intrusion and Trespass	Priority
Drone observed flying every day for a week near Kent State University airport	**P2**

Summary

A drone was spotted flying every day between 8:00pm to 8:30pm for a week in the vicinity of the airport.

Overview

During the past week, aviators at Kent State University airport have spotted a drone flying consistently between 8pm to 8:30pm in the vicinity. The drone was spotted to have flown above the allowable height ceiling of 400ft and, although the airport had no intention to press charges against the drone operator, a police report had to be made due to possible safety and flight implications. The airport understands that Kent State University offers drone and aerial photography courses and suspect most drone operators may be students undertaking the modules. The incident had never happened before, and the university was notified to remind their students on the laws of drone operations.

Analysis

With the rise in use cases of drones, more people are seeing the benefits of drones as part of their business activities or as a hobby. However, it is also very easy for drone operators to get fixated on flying the drone that they may have accidentally infringed regulations set for drone operations. Newer drones and their controllers may visualise and operate within boundaries set by manufacturers; however, these No-Fly Zones (NFZ) may be easily bypassed or manipulated with basic modding or system bypasses.

Drone laws and airspace restrictions are set in place for safety reasons and protection of manned aircrafts and pilots. Drone operators should be cognisant with the laws of their country and have the appropriate licenses if required. 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.

Recommendation

Remote Identification and UAS Traffic Management (UTM) systems are a proactive approach to managing incidents between drones and manned aircraft. These systems will allow aviators and law enforcement agencies to (if supported by CUAS activities) prevent further navigation by drones which have infringed regulations. These counter drone measures can aid to enforce safe coexistence of unmanned and manned aircrafts, reducing the risk of safety infringements and potential loss of life.

While it may not be possible yet to provide city-wide coverage of drone detection and counter-drone systems, basic preparation measure can be set in place to respond to such incidents. A drone management plan and Standard Operating Procedure (SOP) should be drafted to govern the methodology in handling rogue drones. Enforcement agencies can also appeal to the help of the public as an eyewitness; it is beneficial to have a process for such evidence, and then carefully curated for collection and logging.

Organisations should also aim to undertake mock simulations to hone their response, improve communication flow between involved agencies and practice logging and monitoring of repeated cases. This practice can aid agencies in responding during time critical scenarios, mitigate inherent risks and surface challenges in communication and regulatory requirements.

References:

https://www.record-courier.com/news/20200615/drone-flying-near-kent-state-airport-causes-concerns

After July 2nd, 2020, featured advisories will be available to paid subscribers only. Contact info@dronesec.com to arrange a demo or visit https://dronesec.com/pages/notify to learn more.

1.3. NEWS AND EVENTS (P3)

US coalition conducts drone strike in Idlib, Syria killing 2 Horas al-Din terror group commanders

https://www.stripes.com/news/middle-east/drone-strike-kills-two-al-qaida-commanders-in-northwestern-syria-1.633757

Houthis rebels weaponising drone operations, raising threat level to regional countries

https://www.thenational.ae/world/mena/the-houthis-have-built-their-own-drone-industry-in-yemen-1.1032847#10

Ukrainian militia take down Ukrainian security forces drone in Lozovoye, Donbass, Ukraine citing electronic warfare and air defense systems

https://mobsearch.net/news/1572951208

R9X, a missile with blades, precision strike by drone on a car in Idlib, Syria

https://www.jpost.com/middle-east/secretive-ninja-sword-rx9-airstrike-reported-in-idlib-631466

Police national drone project operations with DJI Matrice 210 systems continue in Oslo, Norway

https://translate.google.com/translate?hl=en&sl=no&u=https://www.uasnorway.no/dronen-forst-pa-stedet-politiet-testet-unikt-droneprosjekt-i-oslo/

Drones and used in attacks on Saudi Arabia oil industry last year were of Iranian origin

https://amp-france24-com.cdn.ampproject.org/c/s/amp.france24.com/en/20200613-weapons-used-against-saudi-arabia-were-of-iranian-origin-un-says

1.4. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P3)

Unified regulations on drone laws for the European Union will begin in December 2020

https://www.easa.europa.eu/drones-regulatory-framework-timeline

https://augustaabogados.com/wp-content/uploads/2020/06/ENG-Legal-Notice-REG.-UE.-Drones-2020.pdf

Vietnam government sets no fly zone for drones over protected installations

https://thuvienphapluat.vn/van-ban/giao-thong-van-tai/Quyet-dinh-18-2020-QD-TTg-thiet-lap-khu-vuc-cam-bay-han-che-bay-doi-voi-tau-bay-khong-nguoi-lai-444766.aspx

Kenya CAA reduces drone import permit charges to allow more uptake of drone operations

https://www.businessdailyafrica.com/corporate/shipping/More-drones-to-take-to-Kenyan-skies/4003122-5577554-rqnhkcz/index.html

Department of Homeland Security, US, opens for comments on public opinion and acceptance of drone usage by first responders

https://www.federalregister.gov/documents/2020/06/09/2020-12378/understanding-public-perception-and-acceptance-of-first-responders-use-of-unmanned-aircraft-systems

India opens drone registration window again due to public request

https://www.medianama.com/wp-content/uploads/MoCA_Public-Notice_Issuance_of_DAN_08_June_2020.pdf

New European UAS Regulations: General Outline and Updates

https://publicapps.caa.co.uk/modalapplication.aspx?appid=11&mode=detail&id=9135

https://publicapps.caa.co.uk/docs/33/CAP1789%20Edition3%20June2020.pdf

US seeks to change policy on overseas weaponised drone sales

https://www.uasvision.com/2020/06/15/us-to-change-policy-on-overseas-drone-sales/

COTS drones are a huge threat in Middle East war against terrorists (commentary)

https://taskandpurpose.com/news/drone-swarms-middle-east-centcom

Pentagon needs to go faster and slower on unmanned systems (commentary)

https://www.forbes.com/sites/bryanclark/2020/06/11/dod-needs-to-go-faster-and-slower-on-unmanned-systems/#2b9445285cb8

Analysis of the new draft rules on drone operations in India (commentary)

https://www.livelaw.in/columns/unboxing-the-proposed-drone-laws-an-analysis-of-the-new-draft-rules-on-uasdrones-in-india-158487

The Art of War: Concerns about Chinese drones (commentary)

https://www.commercialuavnews.com/security/propelling-the-american-commercial-drone-industry-to-new-heights

Developing an Effective Anti-Drone System for India's Armed Forces

https://www.orfonline.org/wp-content/uploads/2020/06/ORF_IssueBrief_370_Anti-Drone.pdf (PDF Document)

5-G-Enabled Security Scenarios for Unmanned Aircraft: Experimentation in Urban Environment

https://www.mdpi.com/2504-446X/4/2/22/pdf (PDF Document)

1.5. COUNTER DRONE SYSTEMS (P3)

NSO launches Eclipse, a portable platform which detects, takes over and lands rogue drones

https://www.nsogroup.com/Newses/nso-group-launches-drone-defense-system-eclipse/

https://www.nsogroup.com/eclipse/

US Army and PhaseSpace to test system on detecting and tracing drone swarms

https://www.army.mil/article/236381/army_researchers_find_new_ways_to_test_swarming_drones

1.6. UTM SYSTEMS (P4)

Beyond introduces VPN infrastructure for secure drone and UTM connectivity

https://bvlos.pro/

Altitude Angel and Immarsat to develop a portable SATCOM UTM for BVLOS drone operations

https://www.altitudeangel.com/news/posts/2020/june/altitude-angel-inmarsat-offer-air-traffic-management-for-uavs/

Singapore's IMDA, M1, MPA and Airbus to conduct 5G network trials for UAM operations

https://www.imda.gov.sg/news-and-events/Media-Room/Media-Releases/2020/IMDA-M1-and-MPA-to-Conduct-Coastal-5G-Network-Trials-with-Airbus-for-Urban-Air-Mobility-Operations

Honeywell creates new unit for UAS and UAM sectors

https://www.ainonline.com/aviation-news/business-aviation/2020-06-15/honeywell-focuses-new-unit-uas-and-uam-sectors

Drone Surveillance System: The Complete Setup Guide

https://medium.com/flytbase/drone-surveillance-system-the-complete-setup-guide-87b892f818b

1.7. INFORMATIONAL (P4)

Turkish military to receive over 500 kamikaze Kargu drones from STM

https://www.defenseworld.net/news/27215/Turkish_Military_to_Receive_Over_500_Kamikaze_Kargu_Drones_Soon#.XuiCpUBuKhc

Australian Army pilots SkyRanger R70 drone from airborne C-130J manned aircraft via SATCOM

https://news.defence.gov.au/technology/cooperating-launch-fresh-ideas

Gizmodo maps out flight data of Customs and Border Protection Predator drones in USA

https://www.gizmodo.com.au/2020/06/we-mapped-where-customs-and-border-protection-drones-are-flying-in-the-u-s-and-beyond/

West Midlands Walsall Taskforce discover $600,000 weed operation using thermal police drones

https://dronedj.com/2020/06/12/drones-takedown-a-628000-weed-operation-in-the-uk/

Bournemouth PD drone unit spots and arrests juvenile for dropping off narcotics

https://www.bournemouthecho.co.uk/news/18515479.cannabis-bike-seized-police-drone-searches-teenager/

Police drone and canine used in search and apprehension of runaway driver

https://www.nottinghampost.com/news/local-news/drone-footage-shows-suspected-runaway-4206314

Jacksonville Fire and Rescue Department uses DJI thermal imaging drones to help detect hot spots on burning ship

https://twitter.com/JFRDJAX/status/1269051050482454529

AeroVironment receives 9.8M for supply of Raven, Wasp and Puma drones to NSPA

https://investor.avinc.com/news-releases/news-release-details/aerovironment-receives-98-million-raven-and-puma-3-ae-awards

IAI acquires drone manufacturer Bluebird Aero Systems

https://www.calcalistech.com/ctech/articles/0,7340,L-3832433,00.html

ST Engineering receives approval from CAAS to perform aircraft inspections using drones

https://www.stengg.com/en/newsroom/news-releases/st-engineering-receives-first-ever-authorisation-from-caas-to-perform-aircraft-inspection-using-drones/

Couple wrongly arrested over Gatwick drone intrusion received police payout (UPDATE)

https://www.telegraph.co.uk/news/2020/06/14/couple-arrested-gatwick-drone-chaos-receive-200000-payout-police/

An EHang Ghostdrone 2.0 caught fire whilst charging

https://www.lancashiretelegraph.co.uk/news/18512883.blackburn-mans-terrifying-warning-drone-exploded-home/

1.8. DRONE TECHNOLOGY (P5)

DJI demonstrates the new Matrice 300 RTK drone and Zenmuse H20T camera

https://enterprise-insights.dji.com/en/dji-darley-m300-rtk-zenmuse-h20t-live-demo

Wibotic secures $5.7M to build wireless charging system for unmanned robots

https://www.geekwire.com/2020/wibotic-raises-5-7m-boost-wireless-systems-charging-robots-drones/

Drone Rescue Systems develop parachute system for DJI Matrice 210

https://uasweekly.com/2020/06/11/smart-parachute-rescue-system-available-for-dji-m210-series/

Droniq and Sky Drone partners to develop real time command and control for BVLOS drone flight

https://uasweekly.com/2020/06/16/droniq-and-sky-drone-make-bvlos-uas-flights-with-real-time-command-control-possible/

Israel MoD and IAI produces SkysPrinter, a 3D-printed drone capable of flight

https://www.janes.com/defence-news/news-detail/israels-first-3d-printed-uav-takes-to-the-skies

Nine organisations collaborate to lead project on drone swarm infrastructure inspection

https://www.uasvision.com/2020/06/17/3-9m-eu-project-for-drone-swarms-to-inspect-infrastructure/

1.9. SOCIALS (P5)

DJI Mavic Pro shot by .223 calibre rifle, manages to return-to-home

https://dronedj.com/2020/06/15/dji-mavic-pro-rifle-shot/

Alleged near mid-air collision between drone and police chopper in Dominican Republic

https://twitter.com/newsheli/status/1272802691484250114

Drone footage of protest in Brooklyn, New York USA

https://twitter.com/JoshuaPotash/status/1272953510292848645

Dan Halliwell appointed C-UAS officer at National Police Chiefs' Council Counter Drone Unit

https://www.linkedin.com/posts/dan-halliwell-6a6461109_drones-uav-newrole-activity-6678336745915895808-ERmr

Risk, Rhetoric and Reality – a conversation about drone data security (webinar)

Click here to access the link.

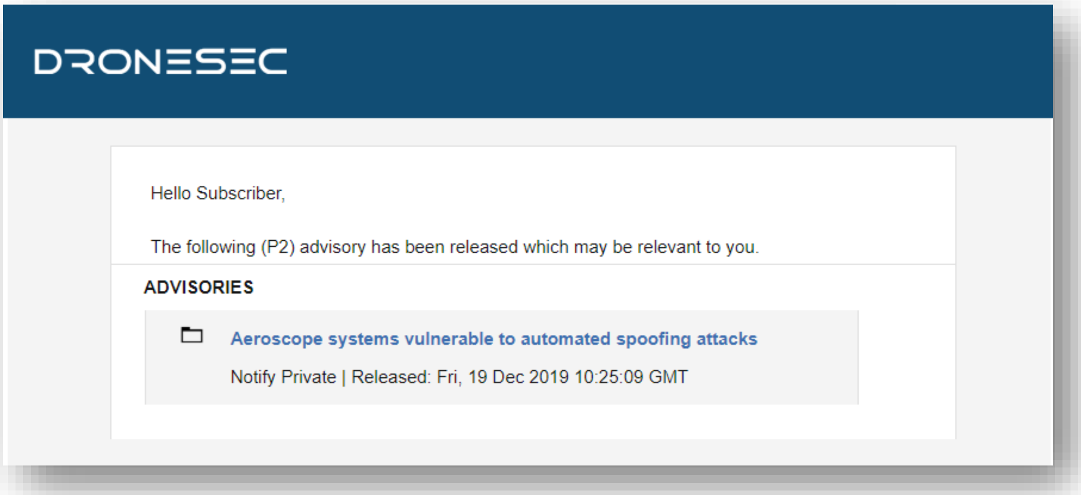
APPENDIX A: THREAT NOTIFICATION MATRIX

A.1. OBJECTIVES

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

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

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



DRONESEC

Hello Subscriber,

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

ADVISORIES

Aeroscope systems vulnerable to automated spoofing attacks

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

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

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

Threat notifications are prioritised based on the following table:

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

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

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

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

Tag - Categories	Description
Drones	Custom-made or Commercial-Off-The-Shelf (COTS) systems that might: • 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.