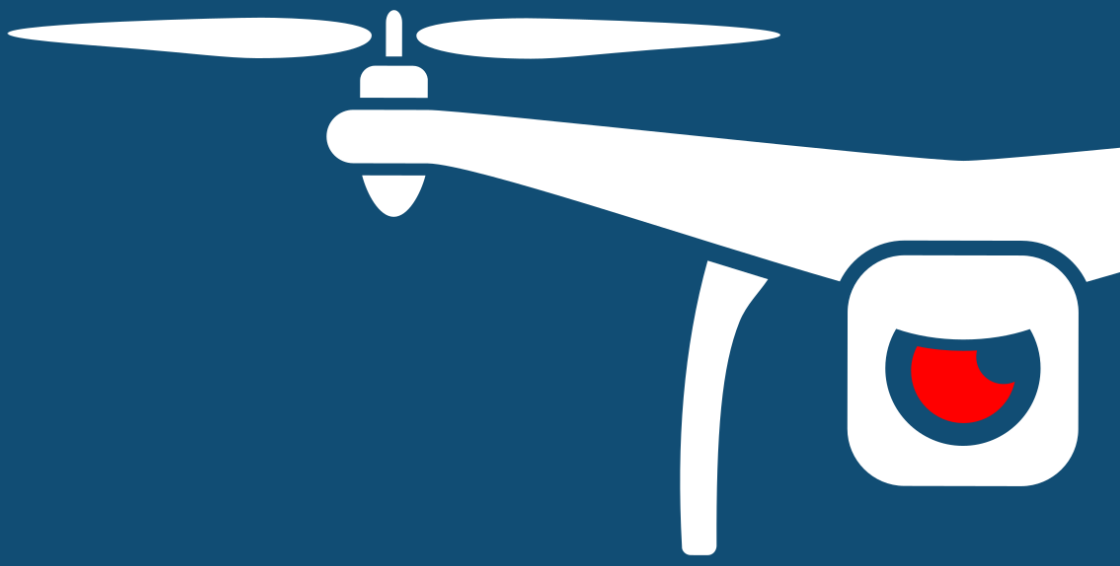
DRONE SEC
A Privasec COMPANY

NOTIFY ISSUE #26

WEEKLY THREAT INTELLIGENCE

11 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

It's not often we see traditional army and military systems used to counter emerging technology threats – often, there is a flashy new system or device. In this week's notify, we cover a new 'smart scope' being used by the US Army to lock on traditional soldier rifles onto fast, low flying unmanned systems. The specific use? Cheap, weaponised adversarial COTS drones in Syria. It reminds me of some work done by researcher Ulf Barth in looking at potential use cases for traditional army camouflage netting in the battlefield as a last-resort physical defence against drones. Sometimes it's important to provide soldiers with items that they're most familiar with, can have easily available and innovate from there.

In the data privacy and security world (our bread and butter), a number of webinars continue the discussion and are only further highlighted by the Booz Allen security assessment report to PrecisionHawk on three DJI drone systems this week. The executive summary of the report is below. The DroneSec team was both surprised and thrilled there are other cyber-security firms tackling the aspects of unmanned systems; we are currently the only firm in APAC that conduct UAS penetration testing services with only several cyber-specific firms in the US spending quality research time and effort in this important industry area.

Overseas, we see continued use of drones by both protesters and law enforcement PDs providing situational awareness for the protests in USA. A $16,000 raid on a DJI store in Manhattan, NY shows looters grabbing as much equipment as they can – almost comically, without controllers in the rush to escape the store with just the base display drone.

In Spain, we see a report providing the various drone incidents per airport, and the related sanction or fines requested and paid. Downing of drones continue on the India-Pakistan border amid new UAS rules referenced for India in 2020 – including the interesting note of drones requiring third-party insurance. From a cyber-security, data privacy and vulnerability aspect, we may soon see drone insurance firms taking these aspects on boars in a similar fashion to pilot error or unintentional crashes.

For all our readers and customers, we hope you and your families keep well as much of the world eases restrictions and once again opens workplaces up post COVID19. We aren't quite at the stage of going back into the office yet (Singapore, Melbourne, Sydney), but I for one am very keen to safely see the team face-to-face again.

- *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.

Kicking it all off, we're delivering our first few rounds in PDF format. In the next few weeks, we'll continue to roll out platform access to ensure we can sustainably support our current client needs with relevant, actionable information within the context of DCU.

Something we missed? Keen to become a supplier? Want to join the Notify platform? Shoot us a message at info@dronesec.com. Otherwise, feel free to hop into the slack channel and introduce yourself: DroneSec Slack Channel. If you missed the previous issue, please email us.

1.2. FEATURED ADVISORIES (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
Pakistan army shoots down Indian-owned DJI Mavic 2 drone which infringed 500m into its LOC	**P2**

Summary

The Pakistani Army announced that they have shot down another quadcopter which infringed into their national boundaries, making it a total of 8 drones this year.

Overview

Even after shooting down two drones in the previous week, the Pakistani border army spotted another quadcopter infringing 500m into its territory. The DJI Mavic 2 drone was spotted and gunned down by the army, making it a total of eight drones in the year 2020 which have infringed into Pakistan from India. The India-Pakistan border have seen frequent drone incursions over the past years due to border disputes. The drone was seized; however, the drone operator was not located.

Analysis

It is well known the conflict between India-Pakistan border groups and that Counter-UAV technology is in use at various points around the Indian side of the border. Both sides record large numbers of drone incidents every month.

Tracked Actor Group:

India-Pakistan Border Drone Smugglers

Motivation and Goals:

- To conduct surveillance, reconnaissance, deliveries and possibly conduct acts of terror

Tactics, techniques and procedures:

- Use of unmanned systems to overcome difficult physical terrain and personnel control barriers
- Use of unmanned systems as a battlefield tactical advantage
- Use of unmanned systems to separate the distance and risk between operators and drone
- Sourcing cheap and available Commercial-Off-The-Shelf (COTS) drones for possible one-way flights
- Self-taught in unmanned and contraband-delivery UAS flights and operations
- Possibly self-taught in engineering and modifying of drone parameter and hardware components
- Recruiting local youths and elderly to conduct a significant number of regular border flights

- Take-off and landing positions in close-proximity border villages and towns over Line-of-Control (LoC)
- Using small and medium-sized COTS drones to deliver munitions (grenades, mortars, small arms weaponry ~<15kgs) to guerrilla groups, often with purchased or home-made dropping mechanisms

Recorded use of drone types:

- Quadcopters, Multi-rotors, Fixed-Wing

Recorded contrabands:

- Ammunition, explosives, counterfeit money, firearms, communication devices, AK-47 assault rifles, grenades

Recorded member groups:

- Khalistan Zindabad Force (KZF) terror group
- Khalistani Jihadi Group
- Khalistani separatists
- Lashkar-e-Taiba
- Jaish-e-Mohammed

Due to the low price-point of these DJI drones, it is possible that they were chosen and used as a one-way mission. In this case, forensic analysis of the drone's telemetry would be incredibly useful, potentially aiding in the launch location of the drone. It is important for law enforcement agencies to have a standard operating procedure (SOP) which aid to govern the process, people and methodology in taking down a drone and collecting forensic evidence of photos and videos stored within.

Recommendation

For huge areas such as border protection, it is understandable counter-drone and drone detection systems are not readily available. Instead, border troops should undertake table-top simulations or exercises to prepare for scenarios like these. Armies should have a Standard Operating Procedure (SOP) or incident response plan in play to govern the process, people and methodology in handling a drone, collecting evidence and responding to potential operators in a pre-determined radius around the protected grounds.

In this case, forensic analysis of the drone's telemetry would be incredibly useful, potentially aiding in the launch location of the drone. All incidents should be logged and categorised. However, as these drones were taken down, the Pakistani Army may expect offenders to take different paths of ingress to avoid detection. Event analysis from the drone data and video footages could assist in recognising patterns and trends (such as origin of flight, time of day etc.) providing possible modus operandi of the operator(s) and may aid in seizure on future attempts of incursions.

References:

https://www.pakistantoday.com.pk/2020/06/06/pakistan-shoots-down-eighth-indian-drone-this-year/

https://twitter.com/OfficialDGISPR/status/1268965058400354310

Security	Priority
17-year-old arrested for collecting narcotics from a drone that crossed illegally from Mexico	**P2**

Summary

A juvenile US citizen was caught attempting to collect multiple packages of narcotics that were dropped from a drone which flew across the US-Mexico border.

Overview

Border Patrol officers from the San Luis US-Mexico border observed a drone dropping packages in the early morning and noticed a male juvenile in the vicinity. The male was collecting and loading the packages into his

vehicle parked nearby. The law enforcement agents arrested the juvenile and found 9 more packages of narcotics, which revealed to be methamphetamine, stashed in the vehicle. The drone and its operator originated from Mexico, but were not seized, however. No further information has been provided.

Analysis

Tracked Actor Category:

Mexico-United States Border Drone Smugglers

Motivation and Goals:

- To supply narcotics to individuals/syndicates with reduced risk of discovery and apprehension

Tactics, techniques and procedures:

- Use of unmanned systems to disassociate operators from contraband.
- 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 possible one-way flights.
- External mechanisms or home-made devices to drop payload, or for attaching contraband.
- Self-taught in unmanned systems and contraband-delivery UAS flights and operations.
- Using drones to drop contraband (narcotics, weapons, possibly up to 7kgs) across borders.

Recorded use of drone and equipment types:

- Quadcopters, Multi-rotors

We are starting to see more drone deliveries across national borders and prisons carrying heavier payloads. Offenders and organised groups realise that law enforcement agencies are starting to take note of illegal deliveries conducted via the use of drones and are continuing to innovate on their delivery methods. To reduce the risk of losing all their contraband and getting caught if the drone was seized, these offenders are turning towards overloading the drones or purchasing a more costly but high weight-capacity drones to reduce the number of delivery runs.

The low price point and availability of COTS drones still make drones an easily accessible tool to conduct illegal acts without too much risk of being apprehended. Offenders are disconnected from the drone by distance and wireless transmissions, however, the risk of being traced due to forensics on video and photo footages is a risk inherent in such operations. Furthermore, with regulations on the need to register drones, it is now harder to purchase drones which are not registered with the aviation authorities.

Recommendation

The San Luis border patrol officers have encountered illegal drone deliveries since 2015 and they have a sound Standard Operating Procedure (SOP) and security management plan for drone infringements. Other law enforcement agencies and organisations should aim to plan for counter-drone response kits and systems to aid in preventing the ease at which such cases can happen. Counter-drone systems, even with just detection mechanisms, can aid security personnel in responding to drone intrusion to prevent unwanted drop offs. A drone security management plan to deal with small unmanned systems should govern the process, people and methodology in handling a drone, collecting evidence and responding to potential operators in a pre-determined radius around the prison grounds.

Any incident should be logged and categorised. Event analysis and monitoring can help law enforcement and forensics agencies recognise patterns and trends which may help in the arrest of the operator. This information can also aid border patrol bodies in practicing and timing their response during an incursion and surface any challenges faced in communication and regulatory requirements.

References

https://www.cbp.gov/newsroom/local-media-release/yuma-sector-arrests-juvenile-retrieving-meth-dropped-cross-border-drone

Intrusion and Trespass	Priority
Two drone incursions over Bighorn fire spot grounding air assets	**P2**

Summary

Firefighters have been hindered in fighting the fire at Coronado National Forest as helicopters were not able to fly due to sightings of drone operations.

Overview

The Forest Service were battling a lightning-sparked forest fire at the Coronado National Forest in Arizona, USA, and engaged the use of helicopters to help extinguish the flame via airborne water drop. However, reports of drones flying overhead the incident site restricted the entry of the helicopter into the area. The Fire and Rescue Service made a public announcement immediately requesting for public to keep their drones away from the area as it was actively hampering firefighting efforts. The drones were sighted but not seized and operators were not caught.

Analysis

Possible Threat Actor: *Hobbyist*

It is now common to observe drone operators flying into restricted areas just to capture a snapshot of the 'action'. However, most of them do not have a full grasp of the scenes that are happening on the ground and the possible coordination of air movement during the event. Rules on drone operation can be found online in the local government aviation websites and mobile applications for the convenience of operators. However, drone operators may not necessarily tune in to local civil aviation websites where Notice to Air Man (NOTAM) may have been issued, restricting the airspace from drone operations. Due to this ignorance, an increase in drone incursions have been happening globally, causing delays in emergency situations and bringing a negative impact on the drone industry.

Drone laws and temporary airspace restrictions are set in place for safety reasons and protection of manned aircrafts and pilots. A study from the FAA also concluded that drone strikes caused more damage to aircrafts and helicopters than bird strikes, due to the hard and rigid components of drones. With the capabilities of drones being able to fly further and higher, these advancements are beneficial when utilised correctly, but cause harm when not adhering to regulations set in place by authorities.

Recommendation

For cases such as this, including medical evacuation where time is of the essence, it is important that these agencies have a drone management procedure with the local enforcement bodies. Simply producing a public announcement requesting operators to stop is often not enough to prevent it from reoccurring. Undertaking table-top simulations or exercises with local enforcement agencies to counter such scenarios aid to mitigate potential delays, overcome landing preventions and quickly involve the appropriate law enforcement bodies to remove the incursion.

Remote Identification and UAS Traffic Management (UTM) systems are a proactive approach to managing incidents between drones and manned aircraft. UTM systems enforce safe coexistence of unmanned and manned aircrafts, reducing the risk of safety infringements and potential loss of life.

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.

References:

https://www.kold.com/2020/06/08/least-second-time-drone-has-grounded-crews-battling-bighorn-fire/

https://www.kold.com/2020/06/09/bighorn-fire-progress-halted-by-drone/

Intrusion and Trespass	Priority
Two Singaporean men charged for flying drones within restricted airspace Gombak Base	**P2**

Summary

Two men, on separate incidents, were charged for flying within a restricted airspace, one within a military base and another within an airbase.

Overview

Neo Wei Ren, 35, was charged with 16 counts for repeatedly flying over a protected Army base without a permit and taking photographs of the base. The DJI Mavic Pro drone was flown from a nearby residential property with a total of seven times. The offender also flew his drone above the permissible altitude on all seven occasions before being caught.

Separately, Lee Soon Tee, 66, was also caught for flying his drone within 5km of an airbase. The drone was not registered with the Singapore aviation authorities as Lee claims that the drone, an Emotion Mavic Drone DJ Pro which was a Chinese-replica of the DJI Mavic drone, was supposedly below 250 grams as stated in the specification sheet, compared to its true weight of 734 grams. Lee lost control of his drone after 2 minutes of flight and it flew into the roof of a wafer substation.

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, despite multiple public broadcasts on the rules for drone operations, there are still many users who choose to fly drones into restricted areas due to ignorance or plain disregard of aviation laws. These acts have a negative effect on the drone industry and may see regulators enforcing more stringent rules affecting the legitimate and commercial drone operators more than the intended offenders.

Recommendation

Drone operators must be cognisant of the laws set in place by their country, otherwise there could be a negative repercussion on the innovation within the drone industry as regulators enforce more stringent rules to clamp down on errant operators. Singapore is one such example where stiffer penalties were invoked in January 2020 to clamp down on errant drone users. Drone laws and no fly zones are set in place for safety and security reasons.

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.todayonline.com/singapore/man-charged-taking-aerial-photos-mindef-gombak-base-after-illegally-flying-drone-above

https://www.channelnewsasia.com/news/singapore/man-charged-flying-drone-take-photos-mindef-base-12818600

Intrusion and Trespass	Priority
Florida man given a trespass warning for flying drone in Disneyland, USA	**P2**

Summary

A drone operator thought it was safe to fly a drone over the currently closed Disney World for an iconic photo but was given a warning as the area was classified as a no-fly zone (NFZ).

Overview

An off-duty Orange County policeman spotted a man standing suspiciously behind trees near an apartment complex and approached the man who was found to be flying a drone. Disney security and the sheriff department were notified, and the man was confronted thereafter. The man thought that he could fly a drone over Disney World and take photo of the Cinderella Castle as the park was closed and empty. There were no populace and he felt it was safe to do so. However, Disney security explained that the park was a no-fly zone enforced by the FAA and no drones were allowed in the vicinity of the premises. The man was let go with a warning and no arrest attempt was made.

Analysis

This is not the first occurrence where we saw drone operators flying into restricted areas just to capture an Instagram-worthy photo or video. While it is fairly common to observe drone operators do so due to ignorance or disregard of aviation law governing drone flights, much cannot be done to detect such acts from happening. It is important that drone operators are cognisant of these aviation laws or the consequences of their actions as a near miss or a direct hit could result in potential fatalities. Places of interest usually have a flight restriction in place to prevent any possible drone-human collision if the drone were to malfunction and fall from the sky.

References:

https://www.orlandosentinel.com/business/tourism/os-bz-disney-magic-kingdom-drone-20200605-sxkopgamqfganfnurnacu4otre-story.html

1.3. CYBER SECURITY (P3)

Booz Allen and PrecisionHawk conduct cybersecurity assessment on DJI Mavic Pro, Matrice 600 Pro and Mavic 2 Enterprise to investigate data security

https://www.precisionhawk.com/blog/unmanned-aerial-intelligence-technology-center-of-excellence-conducts-risk-assessment-of-drone-technology (Executive Summary)

https://www.precisionhawk.com/hubfs/Retest_DJI%20Cybersecurity%20Risk%20Assessment%20Final%20Report_03.31.2020%20Executive%20Summary%20(1).pdf (PDF Report)

https://content.dji.com/no-evidence-of-unexpected-data-transmission/ (DJI Report)

Drone exploitation and NFZ modding bypass site NoLimitDronez returns as 2.0

https://nolimitdronez.com/the-wait-for-v2-is-almost-over

drone-hacks.com software modifications released and demonstrated

https://www.youtube.com/watch?v=1Lk9zM7Ze6U

1.4. NEWS AND EVENTS (P3)

Failed plan to crash-land drug-laden drone causes rioting at Long Bay prison Sydney, Australia

https://www.9news.com.au/national/long-bay-prison-riots-sydney-over-drugs-drone/ae11a75a-5b86-4327-924b-010181e6b0c4

Canadian Transportation Safety Board releases report of Royal Canadian Mounted Police helicopter colliding with their Aeryon Systems SkyRanger R60 in February 2020

https://www.avweb.com/aviation-news/police-helicopter-collides-with-police-drone/

Libyan Army downs UAE's Chinese-made CAIG Wing Loong drone in Sirte, Libya

https://www.middleeastmonitor.com/20200607-libyan-army-downs-uae-drone-in-sirte/

Libyan national Army guns down second Turkish drone in Sirte

https://www.almasdarnews.com/article/libyan-army-shoots-down-2nd-turkish-drone-near-sirte/

Jacksonville police investigate illegal drone near Onslow County Jail, North Carolina, USA

https://www.witn.com/content/news/Police-want-to-ID-man-flying-drone-near-courthouse-571047331.html

Report finds that only 65% of drone operators operate within altitude norms (backdated)

https://droneztogo.com/many-drone-pilots-fly-higher-than-legally-allowed/?fbclid=IwAR2yDurrTlKNfSSIEXYGTCxXjbV8uvFvtyohP0l7IK-CW-3umjX1VsIcVWs

US Customs and Border Protection claim situational awareness intention of predator drone use over Minneapolis during George Floyd protests (update)

https://www.vox.com/recode/2020/5/29/21274828/drone-minneapolis-protests-predator-surveillance-police

1.5. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P3)

Spanish Aviation Authority releases number of drone incidents and sanctions per airport

http://www.senado.es/web/expedientdocblobservlet?legis=14&id=21275 (Spanish – table 2 onwards)

https://translate.google.com/translate?hl=en&sl=es&u=http://www.senado.es/web/expedientdocblobservlet%3Flegis%3D14%26id%3D21275&prev=search (English – table 2 onwards)

US bill, Securing Our Skies Against Chinese Technology Act 2020, seeks to prohibit use of taxpayer funds for Chinese-manufactured drone systems

https://www.mcsally.senate.gov/news/press-releases/mcsally-introduces-bill-to-prohibit-use-of-taxpayer-funds-for-chinese-drones

India releases draft "Unmanned Aircraft System (UAS) Rules, 2020" for comments, includes requirement for third-party insurance

https://defence.capital/wp-content/uploads/2020/06/Draft_UAS_Rules_2020.pdf (English at page 56)

https://www.insightsonindia.com/2020/06/06/unmanned-aircraft-system-uas-rules-of-2020/

Aviation Occurrence Statistics – RPAS incidents and accidents Australia 2010-2019

https://www.atsb.gov.au/media/5777724/ar-2020-014_final.pdf

Ethical use of drones in COVID-19 national emergency response programme (commentary)

https://www.news.uct.ac.za/article/-2020-06-08-ethical-use-of-drones-in-covid-19-national-emergency-response-programme

USA Pentagon tests hypersonic speed loitering munition suicide drone (commentary)

https://www.thedrive.com/the-war-zone/33934/pentagon-has-tested-a-suicide-drone-that-gets-to-its-target-area-at-hypersonic-speed

Airport World 2020 vision for airport and airspace security (commentary)

https://airport-world.com/2020-vision/

Investigation of Drone Vulnerability and its Countermeasures

https://ieeexplore.ieee.org/abstract/document/9108835 (PDF Available to DroneSec Notify Customers)

Privacy-Protection Drone Patrol System based on Face Anonymization

https://arxiv.org/pdf/2005.14390.pdf (PDF Document)

Artificial Intelligence Applied to Unmanned Aerial Vehicles: Impact on Humanitarian Action

https://app.box.com/s/3kcs73pjai5m06945q42wgh80ld5jbh9 (PDF Document)

1.6. COUNTER DRONE SYSTEMS (P3)

U.S. equip rifles with SMASH 2000 sighting system for lock-on firing solution against drones

https://www.stripes.com/us-army-tests-electronic-smart-scope-designed-to-kill-drones-in-syria-1.632263

Reverse Engineering, AI Exploitation and deconstruction of UAVs for Counter-UAS (commentary)

https://nationalinterest.org/blog/reboot/army-has-found-best-method-killing-enemy-drones-160356

Ascent Vision Technologies awarded $16 million for DoD Counter-UAS capabilities for combat

https://ascentvision.com/ascent-vision-technologies-receives-16m-in-dod-contracts-for-imaging-systems/

Anritsu launches AeroShield passive RF Counter-UAS system

https://www.unmannedairspace.info/counter-uas-systems-and-policies/anritsu-launches-aeroshield-passive-rf-detector-counter-uas-system/

Joint Base MDL partners with AeroDefence under $1.2 million DoD contracts, New Jersey USA

https://www.jbmdl.jb.mil/News/Article-Display/Article/2208839/joint-base-mdl-to-partner-with-aerodefense-to-strengthen-drone-deterrence/

Polish army invites C-UAS to Jagodny air training ground for demonstrations, Łuków, Poland

http://www.polska-zbrojna.pl/home/articleshow/31347?t=Antydron-poszukiwany-ale-najpierw-testowanie#

1.7. UTM SYSTEMS (P4)

India grants exception to ANRA Technologies for operating BVLOS drone operations

https://www.anratechnologies.com/home/rules/anra-technologies-and-swiggy-approved-for-bvlos-drone-delivery-operations-in-india/

Foley Square Shopping Center and Deuce Drones collaborates for drone delivery and testing

http://www.gulfcoastnewstoday.com/stories/up-in-the-sky-its-a-bird-its-a-plane-no-its-a-delivery-drone,93867

NASA patent for UAS traffic management win 2020 government invention award

https://www.unmannedairspace.info/latest-news-and-information/nasa-for-patent-for-traffic-management-of-unmanned-aircraft-systems-wins-2020-government-invention-of-the-year/

1.8. DRONE TECHNOLOGY (P5)

Spartaqs develops Prometheus, a camouflage drone that blends into the surrounding

https://www.thefirstnews.com/article/the-invisible-drone-unmanned-aircraft-that-has-chameleon-camouflage-takes-to-the-skies-13205

Canada launches project to better address BVLOS drone search and rescue operations

https://www.auvsi.org/industry-news/kongsberg-geospatial-partners-use-ai-and-uas-improve-search-and-rescue-ops-canada

U.S. Air Force Research Laboratory considers pitting manned fighter jets against unmanned CUAV for possible AI development

https://newatlas.com/military/human-vs-machine-aerial-dogfights-ai-autonomous/

Isreali Hermes 900 UAS sold to Southeast Asian country for search-and-rescue missions

https://www.jns.org/stranded-at-sea-a-high-tech-israeli-drone-will-come-to-save-the-day/

Skydio continues to win US government surveillance contracts amid industry privacy backlash

https://www.forbes.com/sites/thomasbrewster/2020/06/03/funded-by-kevin-durant-and-founded-by-ex-googlers-this-drone-startup-is-scoring-millions-in-government-surveillance-contracts/#59f1a4264e9e

US Air Force seeks UAS ISR/Strike platform, Medium Altitude UAS and MQ-9 weapon system

https://beta.sam.gov/opp/65c412d7879841d7a8d097db4c8b4735/view?keywords=aflcmc&sort=-modifiedDate&index=&is_active=true&page=3

1.9. INFORMATIONAL (P5)

Two Norway companies compete for $200 million maritime drone surveillance contract in EU

https://beta.sam.gov/opp/65c412d7879841d7a8d097db4c8b4735/view?keywords=aflcmc&sort=-modifiedDate&index=&is_active=true&page=3

DJI signs MOU with UNSW Sydney for education, training and talent development partnership

https://www.dji.com/newsroom/news/dji-education-unsw-sydney-partnership

British Transport Police to incorporate drone surveillance over rails to reduce disruptions delays

https://www.edinburghnews.scotsman.com/news/crime/railway-trespassers-be-spotted-drone-2877064

Drone discovers missing hikers in Maroon Bells Wilderness Area, Colorado, USA

https://www.outtherecolorado.com/drone-leads-rescuers-to-overdue-backpackers-in-aspen/

Eagle County PD drones activated in search for missing 3-year-old boy, Colorado, USA

https://www.9news.com/article/news/local/3-year-old-boy-with-autism-missing-in-eagle-county/73-8824b909-66e5-4d3c-8a23-9ac5cf9e4c76

$16,000 worth of drones stolen from Manhattan DJI Store during protests, New York USA

https://nypost.com/2020/06/04/thieves-steal-16000-worth-of-drones-from-manhattan-dji-store/

Grundy County PD apprehend gas station burglars with Mavic 2 drone, Morris, Minnesota USA

www.wcsjnews.com/news/local/two-alleged-burglars-arrested-with-assistance-from-grundy-sheriffs-office-drone-program/article_4117dd80-aa58-11ea-9601-53b442b639bf.html

Vehicle thief located and caught by Belleville Police Service drone team in Brockville, Canada

https://www.intelligencer.ca/news/local-news/drone-used-to-locate-man-teen-arrested-for-threats

Nottinghamshire PD catches fleeing suspect with help of thermal imaging drone, England

https://www.nottinghampost.com/news/local-news/arrest-made-near-railway-line-4190954

NY PD looks to acquire Draganfly drones for COVID-19 amid Connecticut privacy ban

https://www.policeone.com/police-products/police-drones/articles/nypd-considering-pandemic-drone-rejected-by-conn-police-IlmDiwYdsRawat7Z/

Tarrytown NY Fire Department to receive a free Autel Robotics EVO drone

https://riverjournalonline.com/news/tarrytown-fire-department-chosen-to-receive-drone-and-uav-lighting-kit/20380/

US Border Patrol locate three illegal immigrants with AeroVironment Ragven and Puma drones, reflect on 176 flight hours resulting in 474 apprehensions of illegal individuals in six months

https://dronelife.com/2020/06/04/border-patrol-search-drone-finds-lost-women

1.10. SOCIALS (P3)

Alleged U.S. Secret Service drone sighted hovering over Eisenhower Executive Office Building

https://twitter.com/Acosta/status/1267974378597253122

Huntington Beach PD received intel on threats, used DJI Matrice 210, 6x Mavic Enterprise, Skydio 2 and AEE Mach 4 to locate and arrest suspects over George Floyd protests

https://www.linkedin.com/posts/tim-martin-24293764_over-the-past-two-weeks-we-have-been-faced-ugcPost-6675875455653965827-u_3O

Drone spotted flying above crowd during George Floyd protest

https://twitter.com/SuviShinatose/status/1270628390253613056

Protestor drone spotted flying in close proximity to LAPD helicopter, Los Angeles, USA

https://www.facebook.com/groups/1011262722311716/permalink/2681719531932685/


Israeli IAI Searcher II drone shot down in eastern Ukraine

https://www.facebook.com/andrew.burd.79/posts/125971575788679


Drone videos footages on the aftermath of the George Floyd riots in USA

https://www.youtube.com/watch?v=zcYLNHgivkM (Portland, USA)

https://www.bbc.com/news/av/uk-england-suffolk-52951826/black-lives-matter-drone-footage-shows-ipswich-park-protest (Ipswick Park, USA)

https://twitter.com/ABC/status/1270315929616990208 (Hollywood, USA)

Risk, rhetoric and reality: a frank conversation about drone data security (webinar)

https://register.gotowebinar.com/register/3568495082137678348?fbclid=IwAR2whJDSbW00TbqbM1iQ2jTTth373aW9i_D6zIrb55mCbywZBvOhQvo327c

Modified DJI Phantom 4 Pro v2 drone reaches 4.5 kilometres in height (video)

https://www.youtube.com/watch?v=QS5t-yS5PXo

APPENDIX A: THREAT NOTIFICATION MATRIX

A.1. OBJECTIVES

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

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

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

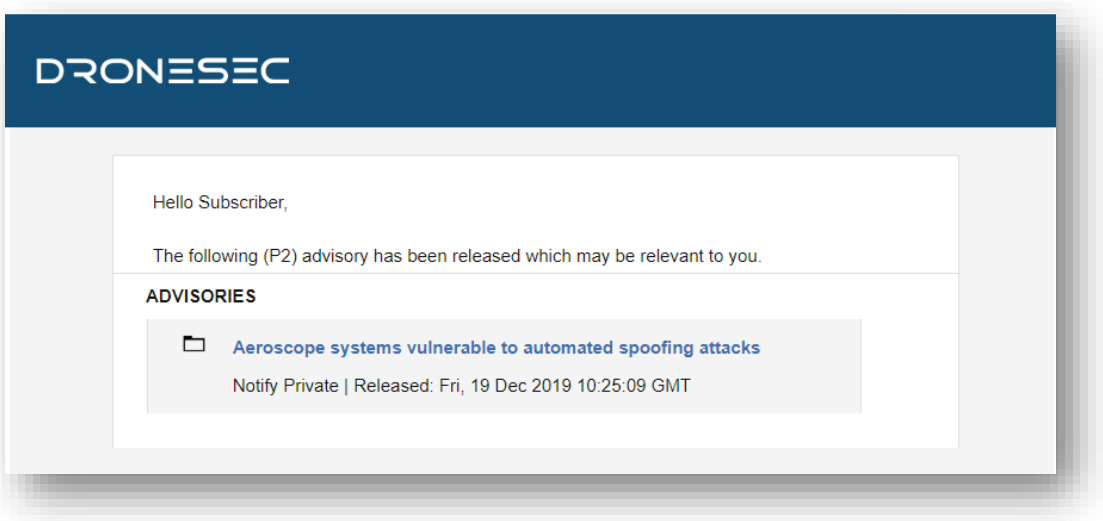


Figure 1 - A threat notification specific to a Notify customer's listed keywords.

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.