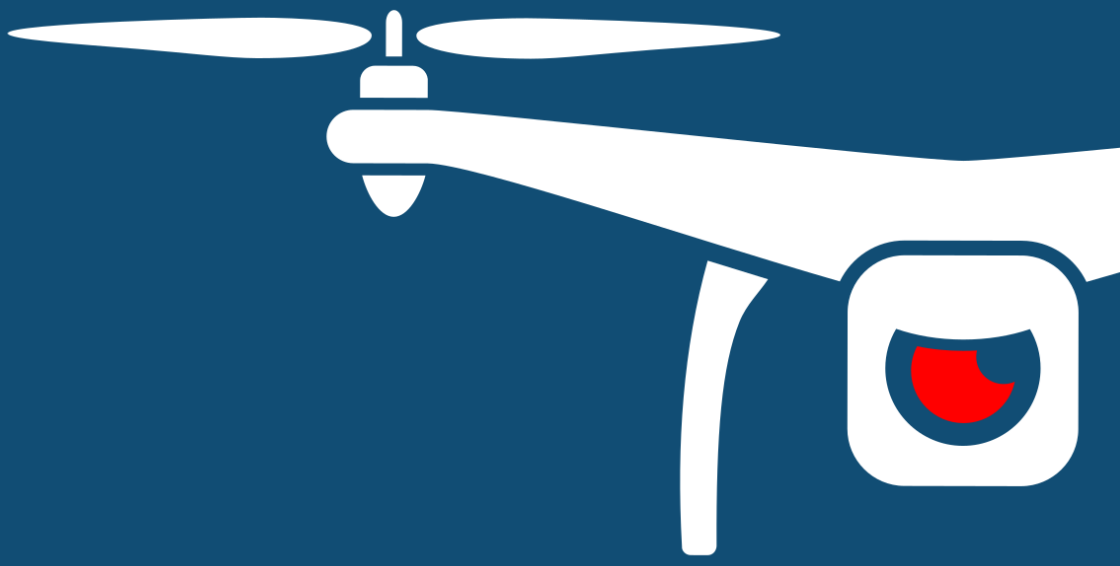
DRONE SEC
A Privasec COMPANY

NOTIFY ISSUE #22

WEEKLY THREAT INTELLIGENCE

13 May 2020 | v1.0 RELEASE



UAS HACKING, HARDENING AND DEFENCE

UAS PENETRATION TESTING
COUNTER-UAS CONSULTING
FORENSICS & INCIDENT RESPONSE
AERIAL THREAT SIMULATIONS
DRONE SECURITY MANAGEMENT PROGRAMS

DOCUMENT **CONTROL**

PREPARATION

DroneSec (dronesec.com)

Threat Intelligence Team

Email: info@dronesec.com

Phone: 1800 996 001 | + 614 7854 3434 (Urgent)

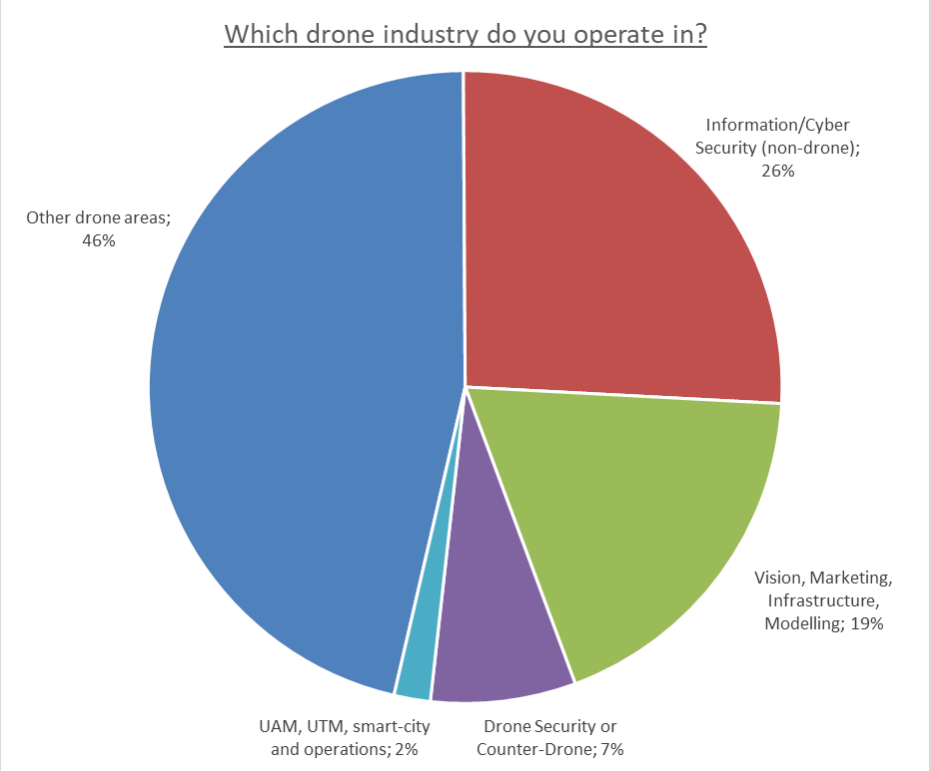
EXECUTIVE SUMMARY

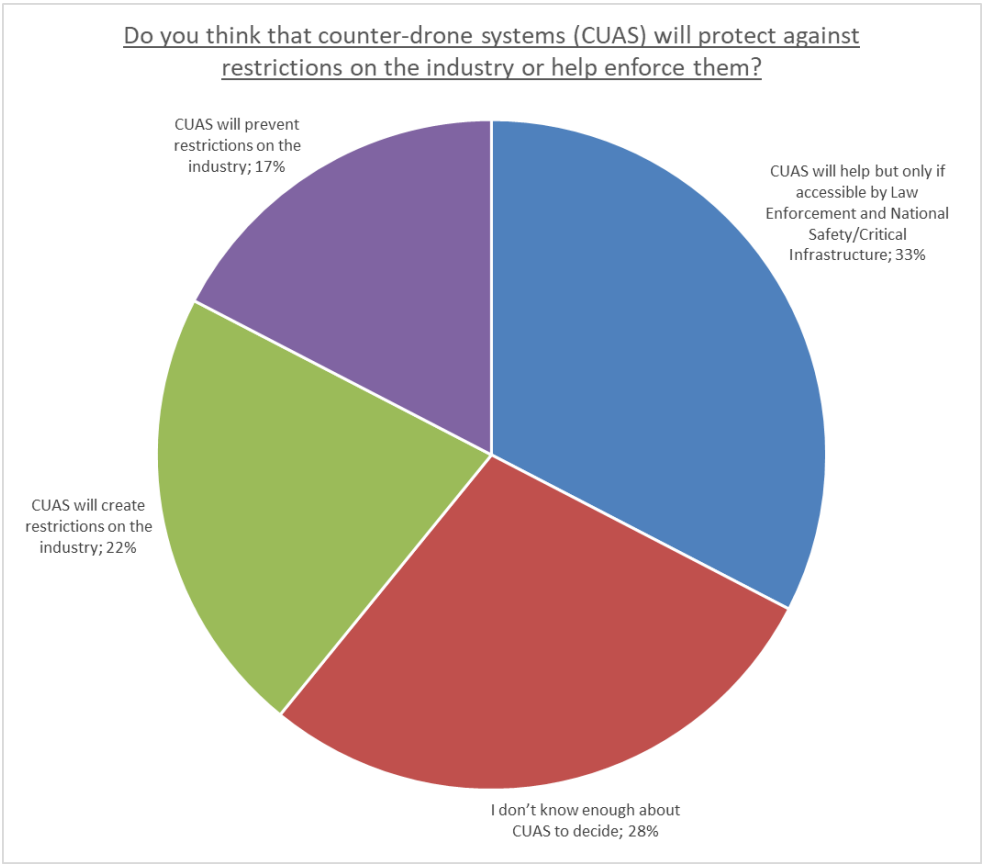
A promising few weeks of flattening the COVID-19 curve here at DroneSec HQ in Melbourne – our hope is that it will be the same for our readers in over a hundred different countries throughout the world.

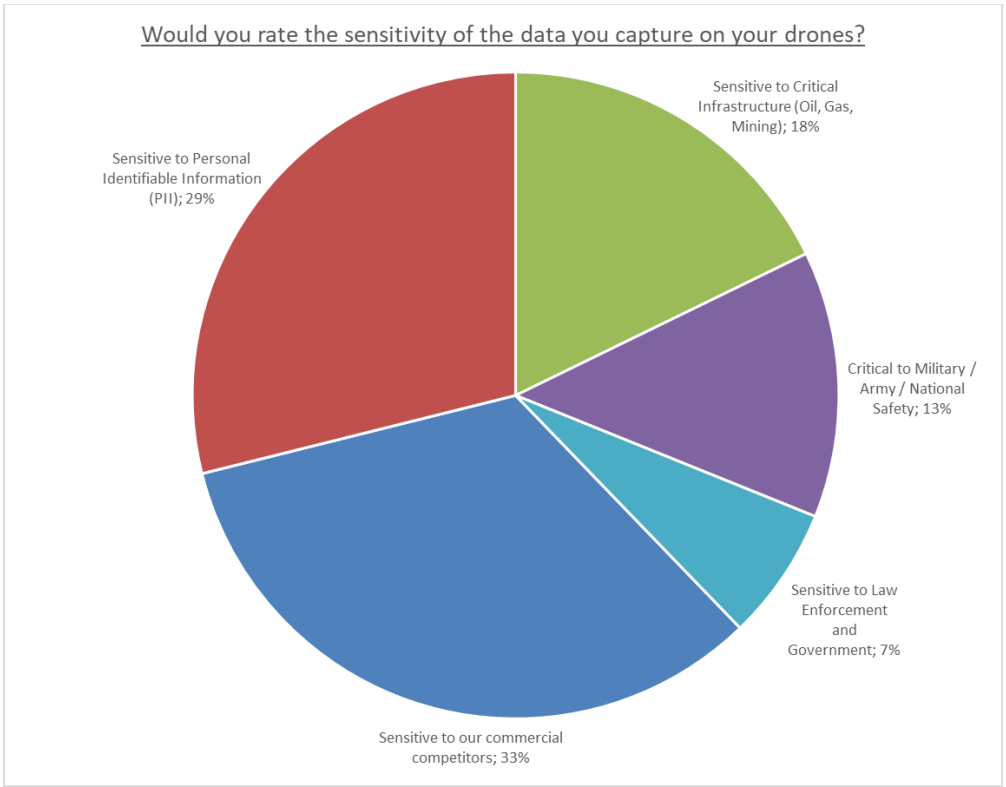
Multiple drug-deliveries via drone make the headlines this week, with many likely kept private for various reasons. A few featured articles this week as we continue to have requests for more information regarding specific events. We see some military drones downed in 'technical and mechanical failures' coming out of the socials.

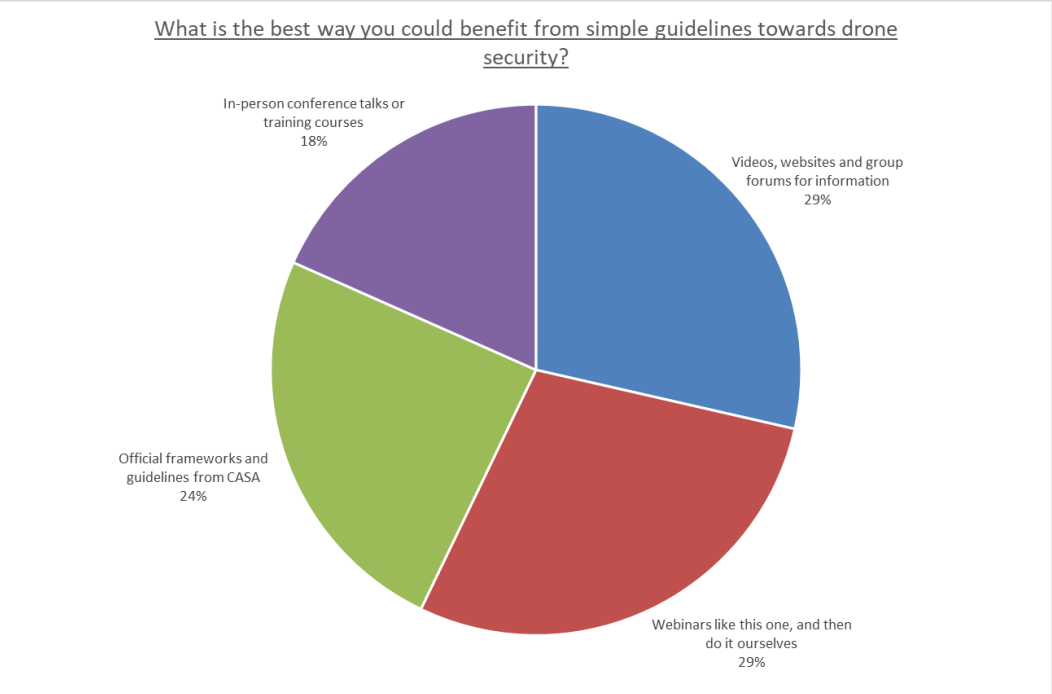
An interest to me this week was the UK governments DASA programme on finding and neutralising small UAS threats. Their document is well laid out and has a *very* informative plan. Specifically, the "What we want" and "What we do not want" clear-cut requirements; this has shown through Bug Bounty programmes to be quite successful in clarifying the immediate while removing signal noise.

Lastly – a few weeks ago we had the pleasure of speaking on a drone security webinar where we asked the audience some poll questions. There was roughly 80 - 100 attendees so the data is thankfully quite comprehensive. Results are below:




Do you think that counter-drone systems (CUAS) will protect against restrictions on the industry or help enforce them?
CUAS will prevent restrictions on the industry; 17%
CUAS will help but only if accessible by Law Enforcement and National Safety/Critical Infrastructure; 33%
CUAS will create restrictions on the industry; 22%
I don't know enough about CUAS to decide; 28%


Would you rate the sensitivity of the data you capture on your drones?
Sensitive to Critical Infrastructure (Oil, Gas, Mining); 18%
Sensitive to Personal Identifiable Information (PII); 29%
Critical to Military / Army / National Safety; 13%
Sensitive to Law Enforcement and Government; 7%
Sensitive to our commercial competitors; 33%



Now – after our Global Drone Security Network (GDSN) launch in Singapore in February, we are putting together the program for our next virtual event. We're combining law enforcement, UTM/UAM, Counter-UAS, Drone Security/Forensics and more; if you'd like to apply to speak or participate (virtually), please get in touch with us at info@dronesec.com. Hope to see/hear some of you on there.

- *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.

Security	Tags	Priority
Phantom 4 drone downed at San Luis border with 700g of drugs, USA	Infringement, Contraband, Border, Seizure, Arizona, San Luis, DJI Phantom 4	P2

Summary

Yuma Sector Border Patrol agents intercepted another drone attempting to smuggle drugs across the San Luis, Arizona border.

Overview

Despite the recent three drone-drug smuggling attempts during the week of April 29th to May 3rd, 2020, the U.S. Yuma Station Border Patrol agents in San Luis recovered a Phantom 4 DJI drone containing two packages of methamphetamine. The drone was found near the New Canal on the west side of San Luis, Arizona, USA. Authorities indicated that the direction of drone suggested it had come from Mexico

Analysis

In this scenario, the act could have been performed by a repeating offender or organised group as the drop off seems to be well coordinated with an undetected approach and egress. The San Luis Border has seen a recent rise in contraband delivery via drones which could indicate that drug cartels have found the feasibility of using commercial-off-the-shelf (COTS) drones as part of their modus operandi. The low price point and availability of COTS drones makes it an easily accessible tool. Without too much risk of being apprehended as drones and operators are separated by distance and wireless transmissions, coupled with a low skill barrier for a successful drone operation, such method of deliveries becomes more lucrative to offenders.

Recommendation

Yuma Sector Border Patrol likely have a drone security management plan in place. Drones were not only spotted but were also taken down thereafter. However, due to the low price-point of drones, it is possible these were 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 handling a drone, collecting evidence and responding to potential operators in a pre-determined radius around the protected grounds.

Likewise, all incident should be logged and categorised. Successful incidents often see offenders becoming lax with their approach and utilising the same take-off/landing points as before. However, as these drones were taken down, the Yuma Border Patrol can expect offenders taking different paths of ingress to avoid detection. Event analysis from the drone data and video footages and recognising patterns and trends (such as origin of flight, time of day etc) may help provide the modus operandi of rogue groups and may aid in the arrest of the operator.

Finally, protected facilities that are in counter drone denied environments (whether regulatory or financially)

should seek detection systems that do not seek to necessarily mitigate but do provide tracking and post-incident analysis capabilities.

References

- https://www.washingtontimes.com/news/2020/may/10/downed-drone-near-arizona-border-had-2-packages-of/

Security	Tags	Priority
Drug dealers in the UK used drones to peddle drugs to avoid being caught	Modding, Contraband, DJI Phantom 4, UK	P2

Summary

In the UK, drug dealers have been found to have resorted to drug delivery via drones to avoid detection and arrest.

Overview

Despite the COVID-19 lockdown, buyers and sellers of drugs in the UK have modified the way drugs are peddled to avoid being spotted and caught in the open on the empty streets. Sellers will now attach bags of drugs onto the drone and have them fly all the way to the buyer without the need for either to leave their homes. Buyers will use bright objects such as towels to indicate landing spots for the seller's drones. Once the deal is completed, both parties will meet later at a supermarket car park for the cash transaction. This new method of operation makes it harder for local enforcement officers to spot such activity and greatly reduces the risk of drug peddlers being arrested. The UK police are aware of these methods, however, peddlers are always finding new ways, such as dressing up as key workers during this lockdown, to continue their sale of drugs.

Analysis

There have been multiple occurrences of drone deliveries into restricted areas like prisons and across borders. Using drones is a cost-effective and risk-reduced technique without being spotted and allows operators to distance themselves from the desired drop site which could have patrol officers on guard. Drones allow malicious users to operate safely with a low risk of being apprehended by law enforcement agencies due to being disconnected from the threat. 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 from plain sight. Operating the drone itself has a low skill barrier and drug peddlers tend to get away easily as many common public areas do not possess drone detection or counter drone systems to prevent the delivery from happening.

Recommendation

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 process, people and methodology in handling a rogue drone.

Enforcement agencies can also appeal to the help of the public as an eyewitness; it is beneficial to have a

process for, and then carefully collect evidence for collection and logging. This data can help to determine if the drone was similar to previous cases which may help provide the modus operandi of drug peddlers and assist in the arrest of the operator.

Organisations should also aim to undertake mock simulations such as reacting to payload-based drone incidents to hone their response, improve communication flow between emergency and rescue agencies and practice logging and monitoring of repeated cases. This information can aid law enforcement agencies in practicing and timing their response, mitigate risk and undergoing challenges faced in communication and regulatory requirements.

DroneSec offers services in guiding organisations interested in procuring counter drone systems, drone threat intelligence within their environment, setting up frameworks on drone incidence response, or simply educating on drone operations and security. More information can be found at https://www.dronesec.com or email at info@dronesec.com.

References

- https://www.mirror.co.uk/news/uk-news/cocaine-dealers-delivering-drugs-drones-22001448

Security	Tags	Priority
Man found hiding in bushes arrested for operating drone near prison, UK	Infringement, Prison, Security, Apprehension, UK	P2

Summary

A man was found hiding in bushes after reports made regarding a drone flying in the vicinity of the Prison.

Overview

After a series of reports from citizens that drones were being flown in the area near a prison in the UK, the Lancashire Police were alerted and found a drone operator responsible for the act. The man was hiding in the bushes to avoid arrest but was found and caught.

Analysis

Although not standardised, public community information can aid in the arrest of rogue drone operators in counter drone denied environments. The help of the public as an eyewitness is beneficial for local enforcement agencies and these reports can be processed and logged to help determine if the drone was similar to previous cases. This evidence can lead to the discovery on the modus operandi of rogue drone operators and assist in the arrest of the operators.

With the rise in use cases of drones, more people are seeing the benefits of drones and have bought one to test out its effectiveness, for business or as a hobby. However, despite multiple public broadcasts on the rules for drone operations, there are still many users who fly drones into restricted areas due to ignorance or plain disregard of aviation law. These acts have a negative effect on the innovation within the drone industry as regulators will enforce more stringent rules to clamp down on these errant operators – sometimes, affecting

the legitimate and commercial drone operators more than the intended party.

Recommendation

For law enforcement bodies or prisons where counter-drone systems are not readily available, undertaking table-top simulations or exercises to counter for scenarios like these are essential. Training is recommended for operators working in a field that could be affected (both directly and indirectly) by rogue or disruptive drones.

DroneSec offers services in guiding organisations interested in procuring counter drone systems, monitoring drone threat intelligence within their environment, setting up frameworks on drone incident response, or simply educating seasoned and newcomers with training courses on drone operations and security. More information can be found at https://www.dronesec.com or email at info@dronesec.com.

References

- https://www.lancashiretelegraph.co.uk/news/18441662.police-drone-finds-person-hiding-hedges/
- https://twitter.com/LancsTacOps/status/1259895069777235968

Security	Tags	Priority
Three men arrested for flying a drone over NHS hospital in Scotland	Infringement, Hospital, Security, NFZ, Apprehension, UK	P2

Summary

Three men were charged for flying over NHS Louisa Jordan COVID-19 hospital despite a warning on drone flight restrictions.

Overview

In view of the neighbouring heliport, a temporary airspace restriction was placed upon NHS Louisa Jordan Hospital which was designated as a COVID-19 hospital during this pandemic. However, three men were caught for breaching this restriction and flying a drone above the hospital which could have delayed medical evacuations, put nearby manned helicopters or lives within the hospital at unnecessary risk.

Analysis

It is now fairly common to observe drone operators flying into restricted areas due to ignorance or disregard of aviation law governing drone flights. Despite public broadcast on what can and cannot be done legally with drones, there are still many operators who continue to disregard these for a variety of reasons. Such acts instead have a negative effect on the drone industry such as regulators enforcing more stringent rules on drone operations.

In addition, temporary drone restrictions are placed because of the possible consequences that may arise form a drone strike with manned aircrafts. Studies from the FAA have shown that drone strikes cause more damage to aircrafts and helicopters than bird strikes. Due to the rigid components of drones, their materials when ingested into an aircraft flew much deeper into the engine and dealt a greater proportion of damage compared to animals. It is important that drone operators are cognisant on the consequences of their actions as a near miss or a direct hit could result in potential fatalities.

Recommendation

For medical aviation bodies where counter-drone systems aren't readily available, undertaking table-top simulations or exercises with local enforcement agencies to counter for scenarios like these are essential. Furthermore, they should have a Standard Operating Procedure (SOP) or Incident Response Plan in play to mitigate potential delays, overcome landing preventions and quickly involve the appropriate law enforcement bodies to remove the incursion.

Training is essential for non-operators working in a field that could be affected (both directly and indirectly) by rogue or disruptive drones.

References

- https://www.bbc.com/news/uk-scotland-glasgow-west-52593322

Security	Tags	Priority
Woman and teen caught with drugs and a drone near Wymott Prison	Infringement, Wymott Prison, Contraband, Security, Apprehension, UK	P2

Summary

A woman and a teenage boy were arrested near a prison for possession of drugs and a drone with intention to supply.

Overview

Prison patrol officers were near the perimeter of HMP Wymott prison near Leyland in the UK spotted a car parked near the security fence. Two people were seen running away from the car before a chase was given and they were arrested shortly after. The woman and teenage boy were found in possession of Class B drugs with intent to supply, a drone and both were also suspected for car theft. The investigation is still ongoing and no further information was released.

References

- https://www.chorley-guardian.co.uk/news/crime/woman-and-teenager-arrested-after-drugs-and-drone-are-found-outside-prison-near-leyland-2849149

Security	Tags	Priority
Drone with suspected drug package seized after landing outside Bovingdon prison grounds	Infringement, Bovingdon Prison, Contraband, Security, UK	P2

Summary

Two packages of suspected drugs were retrieved after a drone landed outside a prison in the UK.

Overview

After a drone landed just outside the grounds of a prison in Bovingdon, UK, prison police officers were able to retrieve the rogue drone with two packages of drugs attached to it. The incident happened in the early morning and investigation for this incident was still ongoing.

References

- https://www.hemeltoday.co.uk/news/crime/police-seize-drone-containing-suspected-drug-packages-near-bovingdon-prison-2845007

Security	Tags	Priority
Drone pilot arrested for confessed contraband drop into Longuenesse prison	Infringement, Security, Longuenesse Prison, Apprehension, France	P2

Summary

French Police from Hazenbrouck arrested two men in connection with harbouring drugs with intention to drop

as contraband into the nearby Longuenesse prison in France.

Overview

Sunday, May 3rd, 2020 at 2:30pm, a vehicle was stopped by police on its way to Pas-de-Calals, Longuenesse prison. The driver fled the scene and was caught on foot. In combination with the drone and cannabis seized in the vehicle, the two males confessed to their intent of dropping the drugs into the prison grounds.

References

- https://actu.fr/hauts-de-france/longuenesse_62525/deux-hommes-soupconnes-vouloir-livrer-la-drogue-par-drone-la-prison-longuenesse_33407533.html

Security	Tags	Priority
Drone intrusion spotted near wildfire in Utah, USA	Infringement, Fire, Sighting, Utah, Emergency Services, USA	P3

Summary

While fighting a wildfire in Saddle, Utah, firefighters spotted a drone intrusion near the vicinity.

Overview

While the Utah Firefighting Department were attending to the recent fire in Saddle, USA, which burnt more than 200 acres of land, a drone was spotted near the vicinity of the wildfire. The Utah Division of Forestry, Fire and State Lands confirmed that a drone intrusion occurred, and the appearance of the drone could have put firefighters, residents and homes at risk. A public notice was put up to remind all residents that drone operations near wildfires were considered as illegal. The drone nor its operator were caught and investigations were still ongoing.

References

- https://twitter.com/UtahWildfire/status/1260313561563185152
- https://ksltv.com/437280/saddle-fire-100-acres-midway-suspect/

Security	Tags	Priority
Two major drug busts on Chinese border utilising DJI Inspire 2 drones.	Border Patrol, Hangzhou, China, Guanping, Wenshan, DJI Inspire 2, Apprehension	P3

Summary

Border Patrol Agents make two major drug smuggling cases using DJI Inspire 2 drones in Hangzhou, China

Overview

Police officers from the Xishuangbanna Yunnan Border Management Detachment have revealed details on the disruption of two major drug smuggling cases by utilising DJI Inspire 2 drones. Spotting the offenders from above, the operators coordinated with police on the ground, apprehending three of the alleged suspects.

In total, 26 kilograms of both heroin and methamphetamine were seized from the smugglers. The Border Control department has announced full-time use of the "drones with big data" due to the geographical terrain of the area being large, complex and difficult to traverse. The drones are used on a daily basis to inspect jungle paths, rural villages and border seal facilities for illegal activity.

References

- Community Submission (Clear Sky UAV Security)

1.3. NEWS AND EVENTS (P3)

German military considers weaponizing their drone fleets

https://www.dw.com/en/german-military-considers-using-armed-drones/a-53395829?maca=en-linkedin-sharing

DASA launches Phase 2 - Countering Drones, finding and neutralising small UAS threats

https://www.gov.uk/government/publications/countering-drones-finding-and-neutralising-small-uas-threats-phase-2

https://www.gov.uk/government/publications/countering-drones-finding-and-neutralising-small-uas-threats-phase-2/competition-document-countering-drones-finding-and-neutralising-small-uas-threats-phase-2

Pathfinder programme will allow Coastguards to use Hermes 900 drones in all airspace classes

https://www.suasnews.com/2020/05/the-uk-drones-pathfinder-programme-announces-new-pathfinder-led-by-the-maritime-and-coastguard-agency/

U.S. troops uses COTS drones to train and review Iraqi troops' tactics in combating ISIS

https://www.stripes.com/news/middle-east/us-special-operations-troops-turn-to-drones-to-remotely-advise-iraqis-1.628337

Drones and K9 deployed to locate motorcycle thief, Grants Pass, USA

https://www.kdrv.com/content/news/Police-use-drone-K9-to-track-down-suspected-motorcycle-thief-in-Grants-Pass-570405921.html

Wiltshire Police visits drone owners to remind them about backyard drone privacy breaches

https://www.independent.co.uk/news/uk/crime/coronavirus-lockdown-uk-drones-illegal-use-police-wiltshire-west-mercia-a9507376.html

Thermal sensing drone deployed by Lincolnshire PD observes runaway suspect in building

https://www.lincolnshirelive.co.uk/news/lincoln-news/police-drone-crash-lincoln-traffic-4122263

Skynode seeks to overcome American Drone Security Act 2019 with Auterion

https://www.zdnet.com/article/the-secret-recipe-for-a-commercial-drone-revolution/

Moscow-based, Russian drone modding company SkyHack.RU releases new DJI NFZ bypasses

https://www.skyhack.ru/hacking/

1.4. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P3)

Unmanned System organisations co-sign with aviation against USA FCC Ligado decision

https://insidegnss.com/lead-up-to-impending-ligado-decision-started-with-10-years-of-testing-and-controversy/

Security Analysis of Drones Systems: Attacks, Limitations, and Recommendations

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7206421/ (PDF)

UAV sensor spoofing detection algorithm based on GPS and optical flow fusion

https://dl.acm.org/doi/pdf/10.1145/3377644.3377670?download=true (PDF)

Software-defined networking for unmanned aerial vehicular networking and security: A survey

https://kopernio.com/viewer?doi=10.3390%2Felectronics8121468&token=WzE2MjExMzMsIjEwLjMzOTAvZWxlY3Ryb25pY3M4MTIxNDY4Il0.XdbM0DEZo0-rHhUZUF3ATAPqoVE (PDF)

A Survey on Cyber Security of Unmanned Aerial Vehicles

http://cjc.ict.ac.cn/online/onlinepaper/hdj-201957200011.pdf (PDF)

1.5. SOCIALS (P3)

Lebanese military announce Isreali military drones identified 8 times over the border

https://twitter.com/IntelTweet/status/1260249266523713537?s=20

https://twitter.com/IntelTweet/status/1258471915666145288?s=20

Four GNA Al-Wefaq government fighters killed in LNA UAV strike on Abu Quarain, Libya

https://twitter.com/AJABreaking/status/1259956428858634241

Russian Special Forces operating drones near La Guaira, Caracas, Venezuela

https://twitter.com/ReutersVzla/status/1258856913439207427?s=20

https://lta.reuters.com/articulo/venezuela-politica-seguridad-rusia-idLTAKBN22K2P5

https://www.voanews.com/americas/report-russian-troops-help-venezuela-search-members-failed-incursion

US Military loses drone over Agadez, Niger, citing "mechanical breakdown – no hostile action"

https://twitter.com/aBamako/status/1258423418850103298?s=20

Iranian-made drone lost over Idlib, Syria, citing "technical malfunction" due to wind

https://twitter.com/mohmad_rasheed/status/1258173268286201857?s=20

Australian Army shares their Drone Racing Team Division's footage of army tank training

https://www.facebook.com/AUADRT/videos/vb.157664578142371/255182662506714/?type=2&theater

1.6. COUNTER DRONE SYSTEMS (P4)

U.S. Army to get Raytheon upgraded counter-drone weapons system for small drone threats

https://www.foxnews.com/tech/army-flying-explosive-gets-new-warhead-radar-destroy-drones

C-UAS philosophy and needs dictate system advancements (Commentary)

http://mil-embedded.com/articles/c-uas-philosophy-and-needs-dictate-system-advancements/

1.7. UTM SYSTEMS (P5)

CAL Analytics awarded US$1.6M to develop UTM Contingency Management Platform

https://nuair.org/2020/05/01/drone-integration-work-continues-at-new-york-uas-test-site/

FAA announces partners for developing Remote ID requirements for suppliers

https://www.faa.gov/news/press_releases/news_story.cfm?newsId=24956

1.8. DRONE TECHNOLOGY (P5)

Researchers design drone based on mosquito's collision avoid sensory antenna

https://www.sciencemag.org/news/2020/05/watch-mosquito-inspired-drone-light-and-avoid-crash

US Air Force launches "Agility Prime" program to bring flying cars into reality

https://www.agilityprime.com/#/

https://www.aviationtoday.com/2020/04/28/agility-prime-air-force-commits-winning-innovation-war-electric-vtol-aircraft/

1.9. INFORMATIONAL (P5)

Bahrain PD deploys Inspire drone to enforce social distancing and limit crowds

https://www.zawya.com/mena/en/life/story/Bahrain_using_drones_in_virus_fight-SNG_174094443/

Walton County requests drone mapping on wildfire with Center for Disaster Risk Policy, USA

https://www.wjhg.com/content/news/Drones-used-to-assess-damage-of-Walton-County-wildfire-570339361.html

FAA launches Unmanned Aircraft Systems Collegiate Training Initiative (UAS-CTI)

https://dronelife.com/2020/05/04/faa-drone-training-initiative-announced/

Dive Delivery to trial drone deliveries in San Mateo and Contra Costa with Phantom 4, USA

https://sanfrancisco.cbslocal.com/2020/05/07/drone-home-delivery-service-trial-san-mateo-contra-costa-counties/

ACCIONA uses Matrice 600 to map digital models of tunnels for mining projects

https://www.acciona-me.com/pressroom/news/2020/may/acciona-is-using-drones-during-the-tunnel-construction-phase-to-obtain-digital-models/

Skyports providing 17km medical delivery runs with drones in UK

https://www.obantimes.co.uk/2020/05/08/drones-to-fly-hospital-kit-between-oban-and-mull/

PG&E to conduct electrical and natural gas infrastructure inspections using DJI Matrice drone

https://mendovoice.com/2020/05/pge-to-conduct-electrical-inspections-with-helicopters-and-drones-in-mendocino-and-humboldt-this-month/

Drone delivery with Wing begins in Christiansburg, Virginia USA

https://www.walgreensbootsalliance.com/news-media/our-stories/during-covid-19-drone-delivery-is-really-taking-off

Ireland to roll out trials for drones to spot and help combat wildfire

https://www.irishtimes.com/news/environment/parks-and-wildlife-agency-to-deploy-drones-as-firefighters-eye-in-sky-1.4251938

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.

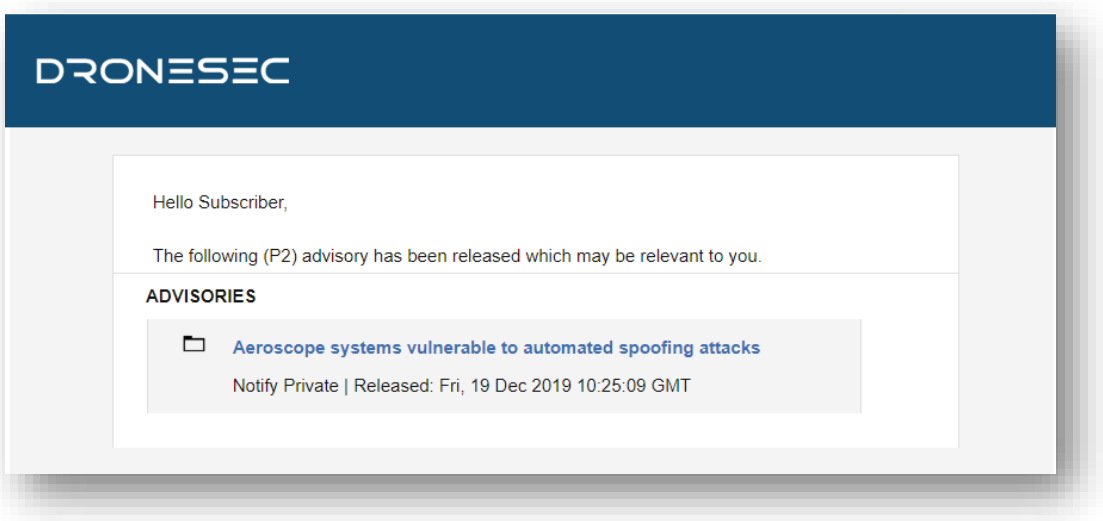


Figure 1 - A threat notification specific to a Notify customer's listed keywords.

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.