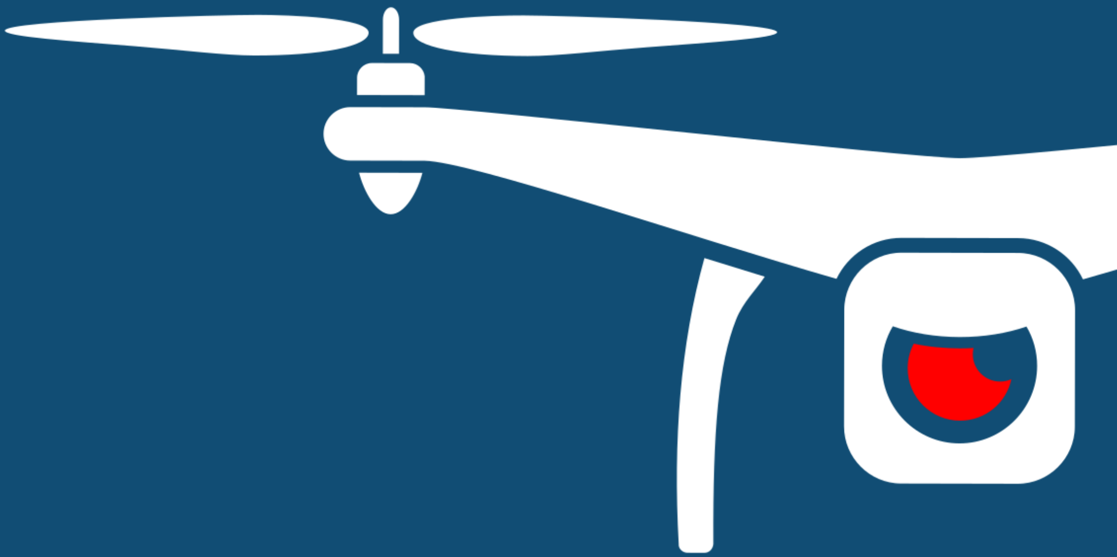
DRONE SEC
A Privasec COMPANY

NOTIFY ISSUE #23

WEEKLY THREAT INTELLIGENCE

20 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

Did you know that between late 2019 and February 2020, CASA, in support of Air Services Australia and the Department of Defense, rolled out 29 passive drone detection systems across **all** of Australia's civil aerodromes? These counter-drone surveillance trails are not new. Trials have been conducted at the MotoGP, Vivid Festival and on the Sydney harbour bridge, but with some interesting statistics coming to light.

Speaking at the AAUS RPAS in the Skies conference (virtually), CASA CEO Shane Carmody announced that 35,000 unique drone systems had been detected across Australian aerodromes in the trials. In the month of March alone, CASA saw 8,468 distinct drones, with some airports such as Melbourne and Sydney receiving over 1,000 each. That's roughly 32 rogue drone detections *per 24 hours*. Now imagine prisons, military bases and more. A commendable effort to the Australian government and interesting to see where the 24/7 real-time feed to the Aviation Services Coordination Center will roll out.

Some of the highlights of this week include a publication titled "*Are drone swarms' weapons of mass destruction*" and "*A report on the use of drones by public safety agencies*". Both of these complex discussion points and well worth the reading material. Moving on, there is a post regarding US Special Operations Command equipping troops with drone-killing drones and a positive to see the New York UAS/UTM test site integrating Cyber-Security as a core implementation component to their UTM contingencies trial.

In the ongoing discussion around data privacy and security, DJI has released a post-mortem analysis of the incident in New York where a DJI quadcopter collided with a Black Hawk helicopter. A must read for forensic and incident responders, be it with all bias or absolutely none; these links are all in the body.

We continue to place emphasis on tracking the individuals, groups or actors behind drone incidents. You will now notice we've started including some of these actors and their Tactics, Techniques and Procedures (TTPs) within the analysis section of certain featured articles. It is important to remember that the drone isn't the threat – it's the people behind them, their motivations and goals a leading battle we must continue to try and stay ahead of.

I'd like to thank URSA Secure for their continued dedication and contributions to DroneSec, Notify and the unmanned forensic and incident response sector in general. In other news, we released an Counter-Drone educational curriculum for high schoolers and drone courses; we're lucky to be partnering with Drone Tech UAS in New York and several other providers to follow. This is an important topic for the great minds of the next generation – who knows, some might be thinking "*I want to be a C-UAS operator when I grow up!*" In reality, teaching safety and security will ensure less restrictions on the industry, and improved innovation.

Our Global Drone Security Network event is lined up for the 10th of July (virtually) – with a great accolade of drone security and counter-drone speakers to discuss the things you simply can't google today. If you're interested in speaking or partnering with us at this event, please get in touch at info@dronesec.com.

- *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
Arrest of ISIS member reveals attack plan to bomb Camp Nou Stadium with drone	Explosive, Drone Strike, ISIS, Barcelona, Spain, Apprehension, Non-Seizure	P2

Summary

A self-professed ISIS member revealed plans for a drone-based bombing attempt against Camp Nou Stadium, Barcelona in Spain. The target of the football stadium was the 'Clasico' match between teams Barcelona and Real Madrid, as revealed in communication from the apprehended suspect.

Overview

A Barcelona male, Mohamed Yassin Amrani, 33, was arrested for communication with jihadist ISIS members. Thousands of text and email messages on his phone revealed the full scope of his attack plans. In his conversations between members of ISIS on Telegram, who were in Syria, he was taught to use a drone with explosive charges attached and given manuals on making a bomb. Amrani was also taught to blend into the crowd and to live a life like a westerner, despite these actions being considered as sinful in Islamic context. Manuals provided to Amrani included how to evade law enforcement bodies and actions to take to avoid being surveyed or caught. Other plans included storming a police station to gun down police officers.

Amrani was classified as a 'lone-wolf' and apprehended, before the incident occurred, by Spanish Intelligence services (SIGC), Morocco's Directorate of Territorial Surveillance (DGST) and the FBI.

Analysis

Tracked Actor Group:

Islamic State of Iraq and the Levant (ISIS)

Motivation and Goals:

- Use of unmanned systems as a battlefield tactical advantage;
- Use of unmanned systems to separate the distance and risk between operators and weaponised payloads;
- Use of unmanned systems to conduct surveillance, reconnaissance and destructive combat missions;
- Use of unmanned systems to cause terror or causalities in urban and civilian environments;

Tactics, techniques and procedures:

- Sourcing cheap and available Commercial-Off-The-Shelf drones for actions aligned with terrorism;
- Extending the range and payload-carrying capacity of COTS drones for malicious missions by modding;
- Training war fighters and soldiers in unmanned and counter-drone UAS flights and operations;
- Using small COTS drones to drop explosive payloads (mortars, grenades ~<600grams) on units below, often with shuttlecocks or home-made flight guidance mechanisms;
- Using custom and purchased amplifiers, transmitters, receivers, antennas, extenders and dual-battery components to improve the overall range and targeting of limitations by OEM systems;

Recorded use of drone types:

- Quadcopters, Multi-rotors, VTOL UAV, Fixed-Wing
- Contact DroneSec for a complete list of custom equipment used by ISIS within unmanned systems

The use of explosive-laden drones by IS/ISIS/ISIL has transitioned from battlefield tactics to use within urban and civilian environments.

Using payload-capable drones is a cost-effective and risk-reduced technique without being spotted and allows operators to distance themselves from the immediate blast radius. 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 until it used to drop the explosive ordinance. Offenders for such acts tend to get away easily as many common public areas do not yet possess drone detection or counter-drone systems to mitigate the threat.

Operating the drone itself has a low skill barrier, however, in this situation, there is some operator experience and domain knowledge required. Investigators managed to collect training materials related to drone use – it is important this documentation is properly analysed and assessed for informing future SOPs.

Recommendation

DroneSec recommends all local law enforcement agencies to be prepared and ready for such threats. 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 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 payload drone incidents to hone their response, improve communication flow between emergency and rescue agencies and practice on the 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.

In the event of 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 rogue groups and assist in the arrest of the operator.

References

- https://www.larazon.es/espana/20200518/gcvb4gytljbihjbsqfdwqapgx4.html
- https://www.thesun.co.uk/news/11651888/isis-fanatic-attack-barcelona-real-madrid-match/
- https://www.rt.com/news/488617-isis-terrorist-clasico-knife-attack/

Security	Tags	Priority
Drone laden with contraband, narcotics located near Forest Prison	Prison, Contraband, Infringement, Seizure, Forest Prison, Belgium, Non-Apprehension	P2

Summary

A drone was found crashed in the vicinity of Forest Prison in Belgium due to overloading of weight caused by the amount of contraband attached to the system.

Overview

In the morning hours, law enforcement officers of the Forest Prison in Belgium found a drone crashed in the vicinity of the perimeter. The drone was carrying drugs and assessed to have been used for illegal delivery of narcotics into the prison. However, the drone could have been overloaded, causing it to fall short and crash prior to arriving at the destination. The Belgium Federal Police is looking into the case and trying to identify the drone operator. No further information has been provided.

Analysis

Tracked Actor Category:

Prison Drone Delivery (Local Disruptors)

Motivation and Goals:

- Use of unmanned systems to supply incarcerated individuals;
- 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;

Tactics, techniques and procedures:

- 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

Illegal drone delivery cases are usually caused by a repeating offender or organised group. The low price point and availability of COTS drones makes drones an easily accessible tool to conduct illegal acts without too much risk of being apprehended as drones are disconnected from the controller by distance and wireless transmissions. Furthermore, the skill barrier to be able to fly a drone is not complex, making it more lucrative to carry out such acts. It is also not easy to trace such offenders as offenders will deliberately avoid registering their drones to prevent detection by law enforcement, reducing the possibility of apprehension.

In this article, the offender may have been too overconfident in the drone's capabilities, overloading it with narcotics rather than sticking to the recommended take-off weight. Overloading the drone will significantly affect the lift, flight duration and speed of the drone as the motors will require more power to sustain operations.

Recommendation

With the rise in cases of contraband deliveries conducted via drones, it is timely for law enforcement agencies and organisations 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 and a Standard Operating Procedure (SOP) 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, categorised and reported to local law enforcement. Event analysis should take place by determining if the drone was similar to previous cases, took similar launch/land flight paths and as much footage of the device captured as possible. Monitoring the drone make and models, 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. This information can also aid law enforcement bodies in practicing and timing their response, undergoing challenges faced in communication and regulatory requirements, and providing investors or stakeholders with assurance as to risk planning.

References

- https://www.breitbart.com/europe/2020/05/16/drone-delivering-drugs-to-belgian-prison-crashes/

Safety	Tags	Priority
Drone hovers dangerously close to Blue Angels acrobatic team	Infringement, Safety, Military, Detroit, USA, Navy	P2

Summary

A video was uploaded onto social media featuring a drone in close proximity of the flyover performance by the US Navy Blue Angels.

Overview

A drone video was uploaded onto social media featuring the flyover performance by the US Navy Blue Angels. The video displayed several angles of the acrobatic display and towards the end of the video, the final shot showed that the left most plane was within extreme proximity to the drone. The FAA and Blue Angels team were made known of this video and thereafter, FAA iterated the rules for a safe drone operation. FAA has began investigating into this matter and the video and social media accounts have been taken down since.

Analysis

DroneSec have a record of the individual and drone used which is not for public release.

This is not the first instance where we had drones flying close to manned aircrafts or helicopters. While it is fairly common to observe drone operators flying into restricted areas due to ignorance or disregard of aviation law governing drone flights, much cannot be done to detect such acts from happening. Remote ID and drone tracking systems may help some, but their effectiveness may be reduced where a racing or FPV drone is involved. Drone operators are not able to accurately assess the height of the drone against the height of the manned aircraft which is one of the key factors in mid-air collision.

In addition, for aerial displays like this, a temporary flight restriction is placed to prevent any other aircrafts from flying into the area. This flight restriction is also applicable for drones because of the possible consequences that may arise from a drone strike with manned aircrafts.

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. Furthermore, regulators may also enforce more stringent rules in an attempt to clamp down on these errant operators – sometimes, affecting the legitimate and commercial drone operators more than the intended party.

Recommendation

Remote ID of drones and UAS Traffic Management (UTM) systems are a proactive approach to managing drones and manned aircraft. UTM systems attempt to enforce safe coexistence of unmanned and manned aircrafts, reducing the risk of safety infringements and potential loss of life. Unfortunately, these systems do not yet provide a comprehensive deterrence and prevention control against all drone types.

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 by finding out any released Notice to Airman (NOTAM) news before commencing their drone operations.

For law enforcement bodies where counter-drone systems are not readily available, undertaking table-top simulations or exercises 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.

References

- https://theaviationist.com/2020/05/14/drone-flies-dangerously-close-to-blue-angels-in-detroit-america-strong-flyover/

Safety	Tags	Priority
Activist drone shot down by shotgun in Butterfield, Minnesota	Crash, Safety, Kinetic, Butterfield, Counter-Drone, Minnesota, USA	P2

Summary

A man who shot down a drone with a shotgun has been charged for the offense.

Overview

A drone operator and activist flew his drone over a food processing company in Butterfield, Minnesota. The operator wanted to observe if chickens were being unnecessarily slaughtered due to the COVID-19 pandemic. However, two employees caught sight of the drone and questioned him on his actions and intent before the drone was then shot down by a shotgun. The drone operator filed a lawsuit against the alleged shooter (Travis Duane Winters, 34) who was charged for damage to property and reckless discharge of weapon. FAA highlighted the illegality of shooting down aircrafts, whether manned or unmanned.

Analysis & Recommendation

Some individuals believe downing drones is justified if privacy or trespass has allegedly been breached. However, the FAA (and other aviation regulators) maintain it is against the law to shoot down any form of aircrafts, whether if it is a manned or unmanned one. Many landowners do not own the airspace above them and are entitled to certain proximity and privacy laws involving drones. These entitlements, however, do not provide an opportunity for reckless use of a firearm in a populated area.

Citizens who feel that their privacy have been invaded due to a perceived infringing drone should always contact their local police department who have a procedure for investigating such cases.

References

- https://arstechnica.com/tech-policy/2020/05/minnesota-man-faces-felony-charges-for-shooting-down-drone/

1.3. NEWS AND EVENTS (P3)

Predator drone crashes on Mathis Field runway due to mechanical failure, Texas, USA

https://sanangelolive.com/news/crashes/video/2020-05-15/cbp-predator-drone-crashed-because-mechanical-issue

Missing drone in Latvia found in forest – drone data being analysed for interference [UPDATE]

https://eng.lsm.lv/article/economy/transport/latvias-runaway-drone-rescued-and-brought-home.a360133/

Iraq's Popular Mobilization Unit shoots down drone belonging to ISIS, denies infiltration attempt

https://iqna.ir/en/news/3471447/daesh-drone-downed-in-iraq's-khanaqin

Lebanese brothers plead guilty for exporting drone technology to terrorist group, Hezbollah

https://www.defensenews.com/unmanned/2020/05/19/lebanese-man-pleads-guilty-to-drone-parts-export-conspiracy/

Organised crime groups using drones to survey football players houses during mid-match thefts

https://www.marca.com/futbol/2020/05/15/5ebc388222601dc56e8b45f9.html

DJI, NTSB analyses post-incident drone and Black Hawk helicopter collision in NY, USA

https://content.dji.com/how-i-know-dji-doesnt-have-your-drone-data/

https://app.ntsb.gov/pdfgenerator/ReportGeneratorFile.ashx?EventID=20170922X54600&AKey=1&RType=HTML&IType=IA%EF%BB%BF

https://security.dji.com/data/resources/

US Army deploy ALTIUS fixed-wing drone from Black Hawk for battlefield applications

https://www.verticalmag.com/news/drone-launched-black-hawk/

DJI Matrice M210 drone crashes into congested pavement area, Hastings UK

https://www.theargus.co.uk/news/18453560.drone-crashed-pavement-hastings/

Residents in South Zone of Rio, Brazil claim drones entering homes through window

https://diariodorio.com/moradores-da-zona-sul-do-rio-reclamam-de-drone-misterioso-entrando-por-suas-janelas/

Autel wins lawsuit against DJI's infringement of its patents filed in 2018

https://www.slrlounge.com/dji-loses-patent-suit-could-be-removed-from-the-us-market/

Singapore Police Force UAV Unit trials drone box system with an off-site command centre

https://www.straitstimes.com/singapore/surveillance-drones-operating-autonomously-take-to-the-sky-in-police-trial

Police drone team raid results in drug bust, Coventry UK

https://www.coventrytelegraph.net/news/coventry-news/police-use-drones-drug-seizure-18265350

Activist drone footage captures hunter ingesting drugs, resulting in arrest, Melbourne Australia

https://www.abc.net.au/news/2020-05-20/victorian-duck-hunter-guns-seized-by-police-after-drugs-found/12264650

1.4. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P3)

Remote ID service targeted for launch in 2021, FAA

https://www.aviationtoday.com/2020/05/14/faa-targets-2021-launch-first-public-drone-remote-id-service/

European Commission updates standards for BVLOS drone operations

https://eur-lex.europa.eu/eli/reg_impl/2020/639/oj

France State Council rules against using drones for monitoring social distancing

http://www.rfi.fr/en/france/20200518-french-court-blocks-use-of-drones-by-authorities-to-enforce-social-distancing

"Are Drone Swarms Weapons of Mass Destruction?" (Publication)

https://www.airuniversity.af.edu/Portals/10/CSDS/monographs/MONO60%20Drone%20Swarms%20as%20WMD.pdf?ver=2020-05-13-135901-057 (PDF Document)

A Report on the Use of Drones by Public Safety Agencies—and a Wake-Up Call about the Threat of Malicious Drone Attacks (Publication)

https://cops.usdoj.gov/RIC/Publications/cops-w0894-pub.pdf (PDF Document)

1.5. COUNTER DRONE SYSTEMS (P3)

Australian Government install permanent passive RPA detection systems in all 29 aerodromes

https://youtu.be/mOKTQzrL1YQ?t=769

U.S. Special Operations Command (SOCOM) to equip troops with drone-killing drones

https://www.ibtimes.com/us-special-operations-command-develop-drone-killing-drones-support-green-berets-2976133

AH-64 Apaches to be upgraded with UAV/drone targeting capabilities

https://www.flightglobal.com/helicopters/us-army-to-receive-ah-64e-version-6-upgrade-with-ship-and-uav-hunting-capabilities-in-august/138363.article

Mont. Ascent Vision Technologies delivers X-MADIS CUAS to undisclosed US defense customer

http://mil-embedded.com/news/x-madis-c-uas-systems-delivered-to-u-s-defense-customer/

Germany technical support tender for national drone detection system closes

https://www.unmannedairspace.info/latest-news-and-information/germany-issues-technical-support-tender-for-national-drone-detection-system-appraisal/

1.6. UTM SYSTEMS (P4)

Altitude Angel releases open-sourced Scout for Remote ID and UTM network

https://www.altitudeangel.com/news/posts/2020/may/altitude-angel-release-open-source-remote-id-scout/

NY UAS Test site for drone UTM integrations such as cyber-security and contingencies

https://www.suasnews.com/2020/05/drone-integration-work-at-ny-uas-test-site/

Boeing to join UK CAA's Innovation Sandbox programme for BVLOS operations

https://boeing.mediaroom.com/news-releases-statements?item=130679

Japan Post completes two-day test for BVLOS parcel delivery

https://www.unmannedairspace.info/latest-news-and-information/japan-posts-tests-bvlos-parcel-delivery-with-view-to-full-operations-by-2025/

Canadian government calls for RPAS traffic management services testing proposals

https://www.tc.gc.ca/en/services/aviation/drone-safety/drone-innovation-collaboration/remotely-piloted-aircraft-systems-rpas-traffic-management-services-testing-call-proposals.html

1.7. DRONE TECHNOLOGY (P5)

Involi launches Kivu, a Remote ID compatible tracker for broadcasting drone ID and location

https://drive.google.com/file/d/1-XCaeUzBS889b5si24ytTrMYFnp-p8cv/view (Press Release)

https://www.linkedin.com/posts/involi_kivu-lakekivuchallenge-kivu-activity-6668461887534981120-hzQL

Parrot partners DroneSense to meet needs of first responders with ANAFI aircraft

https://www.geospatialworld.net/news/parrot-and-dronesense-partner-to-better-equip-public-safety-uas-programs/

Textron Systems awarded US20.7M for development of unmanned naval drones

https://www.spacewar.com/reports/Textron_nabs_207M_contract_modification_for_Navy_drone_program_999.html

ANA and AeroNext collaborate to design a "4D Gravity" separated airframe structure for drones

https://www.drone.jp/news/20200520104042.html

US Navy sees the importance of unmanned systems and the need to prioritise it (Commentary)

https://www.defensenews.com/opinion/commentary/2020/05/15/a-fleeting-advantage-no-time-to-lose-for-us-navys-unmanned-ambitions/

Manned and Unmanned aerial team will be the future of air warfare (Commentary)

https://www.realcleardefense.com/articles/2020/05/13/neither_manned_nor_unmanned_the_future_of_air_warfare_will_be_about_teaming_115283.html?mc_cid=9eecca4013&mc_eid=8c4ab83df3

Singapore roboticists design drones that can spilt into 5 small drones for dispersion of sensors

https://spectrum.ieee.org/automaton/robotics/drones/watch-this-drone-explode-into-maple-seed-microdrones-in-midair

1.8. INFORMATIONAL (P5)

USA Drone Port launch “Spying on America by Foreign-made Drones” webinar series

https://www.bigmarker.com/usa-drone-port/Spying-on-America-by-Foreign-made-Drones

Marine Corps have deficiencies in Electronic Warfare (EW) to counter Unmanned Aerial Vehicles

https://armadainternational.com/2020/05/new-tools-for-new-threats

Homeland Security questioned on DJI provision of drones to law enforcement agencies in the US

https://www-bloombergquint-com.cdn.ampproject.org/c/s/www.bloombergquint.com/amp/business/police-data-on-use-of-chinese-made-drones-demanded-by-lawmakers

Neighbours use drone to search for missing man who fell into Hull Drain, UK

https://www.hulldailymail.co.uk/news/hull-east-yorkshire-news/man-rescued-from-hull-drain-4134606

Natural Resources Wales to work with Gwent Police in using Typhoon H to catch waste criminals

http://www.monmouthshirebeacon.co.uk/article.cfm?id=117896&headline=Drones%20used%20to%20catch%20unscrupulous%20waste%20operators&sectionIs=news&searchyear=2020

West Seneca Police Department to receive R4 Roller drone, New York United States

https://www.westsenecabee.com/articles/police-department-to-receive-drone-at-no-cost-to-town/

Skylark Labs trials AI drones in 6 Indian cities to enforce social distancing

https://www.newscientist.com/article/2243058-us-start-up-is-testing-drones-in-india-to-enforce-social-distancing/

India looks to use drones to combat against desert locusts

https://www.thehindubusinessline.com/economy/agri-business/as-deadly-locusts-go-rogue-drones-are-the-best-way-to-combat-them/article31588989.ece

Braham to consider using commercial drones for mosquito control, USA

https://www.hometownsource.com/county_news_review/news/local/braham-to-purchase-drone-for-mosquito-spraying/article_c34d1064-953a-11ea-872f-6b852480d5f0.html

EagleHawk contracted to use Argas drones to disinfect stadiums and arenas

https://www.inceptivemind.com/eaglehawk-drone-enabled-disinfectant-spraying-stadium-arenas/13252/

Fairfield Firefighters use drone to locate stranded kayaker, USA

https://www.ctpost.com/local/article/Firefighters-use-drone-to-find-stranded-kayaker-15276038.php

Philippines Coast Guard to use drones to monitor coastal settlements during lockdown

https://cebudailynews.inquirer.net/310940/talisays-coastal-patrol-uses-drone-to-monitor-coastal-areas

Portugal Ministry of Environment will acquire 12 drones to survey forest fires

https://www.theportugalnews.com/news/drones-brought-in-to-fight-fire-risk/54119

South Yorkshire Fire and Rescue deploys drones to identify hotspot in Doncaster fire, UK

https://www.doncasterfreepress.co.uk/news/drone-deployed-fire-continues-rage-doncaster-beauty-spot-2858043

Elk Grove Police Department use Mavic 2 drones in law enforcement operations, United States

https://www.abc10.com/article/news/local/elk-grove/elk-grove-police-chief-talks-policing-with-drones-during-the-pandemic/103-eff25694-39a2-4e3a-a52b-8b4f9b2fc4d0

1.9. SOCIALS (P5)

Drone from Gaza infiltrates 200m into Israeli airspace without being shot down

https://twitter.com/manniefabian/status/1260907149066211328?s=20

Israeli Hermes 450 UAV footage capture over Lebanon

https://twitter.com/AuroraIntel/status/1262684924177534976

Downed Haftar terrorist drone was Chinese made (images)

https://twitter.com/BurkanLy/status/1262188801939648513

Wiltshire police UAV team locate missing man with drone, UK

https://twitter.com/danieljaewebb/status/1261766409945841666

Swarm drones used in magic trick in Britain’s Got Talent, UK

https://www.youtube.com/watch?v=JO--pMm22b0

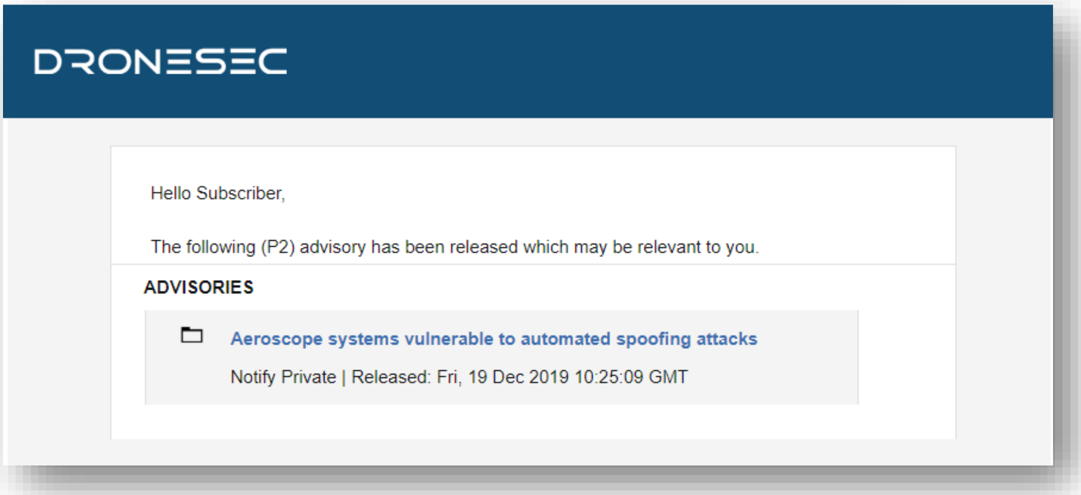
APPENDIX A: THREAT NOTIFICATION MATRIX

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.