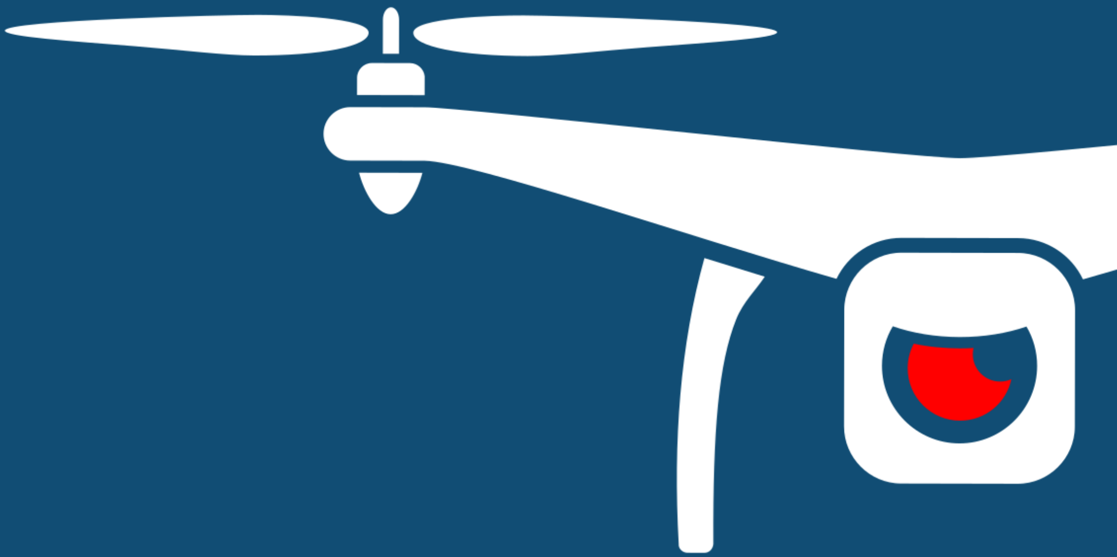
DRONE SEC
A Privasec COMPANY

NOTIFY ISSUE #32 (PUBLIC)
WEEKLY THREAT INTELLIGENCE

22 July 2020 | v1.0 RELEASE



UAS HACKING, HARDENING AND DEFENCE

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

DOCUMENT CONTROL

PREPARATION

DroneSec (dronesec.com)

Threat Intelligence Team

Email: info@dronesec.com

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

EXECUTIVE **SUMMARY**

We are excited to announce that our Global Drone Security Network (GDSN) online event will now take place over a full day. We have various speakers from the CUAS, Law Enforcement, Security Surveillance and Threat Intelligence sectors providing insights into unmanned security-specific topics. We will also be opening up our Call-For-Talk submissions this week for 20 minute and 40-minute talk slots for the few that are left. If you would like to participate in speaking, please send your talk Topic, Description and Bio to info@dronesec.com before the public registration opens up. The event will be free and following its inaugural event in Singapore, is the only of its kind focusing specifically on drone security, counter-drone and cyber-UAV topics.

This week we see a report from the Israel-Lebanon border focusing on a successful hijack and safe-landing of a drone by IDF forces – albeit a drone being flown for hobbyist/commercial purposes. The exact Counter-UAS system is not stated but suggested as being in use. Israel has a number of boutique CUAS vendors, including NSO Group's Convexum and D-Fend Solutions, and large military primes with more of a focus on wartime/battlefield CUAS technologies.

Azerbaijan is regularly increasing in reports of shot-down and jammed UAV's, as are the SMM reports from Ukraine where a number of mini-UAV and long-range UAV's record various levels of GPS jamming and signal interference. Parrot digs its heels into cyber-security with a WISEKEY partnership, with chatter surrounding the potential of a Bug Bounty security program to mirror that of manufacturing rival DJI.

In the UK a report reviews the progress of the 2020 police mobile counter drone unit, and on the other side of the pond the US Armed Services Committee assess whether a "Counter Drone Center of Excellence" would provide greater oversight and support for a skilled workforce entering the CUAS industry. A newly released paper *Review of Counter-UAV Solutions Based on the Detection of Remote-Control Communication* has been released, added to this report and the platform for Notify customers.

Whilst our Singapore office is back open for business, Melbourne is still in Level-3 lockdown with new mandatory mask laws and restrictions on travel. We hope everyone is well and staying safe during this period.

As always, if you have comments or feedback, or want to join in the discussion in our slack group, please don't hesitate to contact us.

- *Mike Monnik, DroneSec CTO*

TABLE OF CONTENTS

1. THREAT INTELLIGENCE

1.1. INTRODUCTION

Threat Intelligence to the DroneSec team means cutting-edge information, news, resources and threats delivered in a succinct and actionable way. Notify is just that – key information that can be used to prepare, prevent and identify threats and challenges which seek to take advantage of the drone industry. Our aim is to allow organisations to make more informed decisions, respond effectively and get a birds-eye view of our core focus: Drones, Counter-Drone and Universal Traffic Management (UTM) Systems – also referred to as **DCU**.

When it comes to proactively seeking out the best solutions, developing response capabilities or building resilience into your drone operations, relevant information is king. We're dedicated to ensuring you stay up to date through Notify, while getting the specific details around techniques, vulnerabilities, targets and malicious actors. Furthermore, we've made all Notify information both scalable and easily categorised, providing a mechanism for easy search but also extraction of statistics and use cases for stakeholders who need pre-mitigation insights and strategies.

For technical operators, we've included the ability to be able to prioritise relevance over noise and communicate with each other to exchange ideas and collaborate on threats. This exchange happens on a number of levels, from our slack channel, to sharing DroneSec case-studies within the platform and hearing from our partners (individuals, technology vendors, law enforcement and regulatory bodies) who supply valuable information to Notify.

Weekly reports are just that – the lifespan only covers one week of intelligence and where this might extend is when we detected or were alerted to it later on. You can rely on this information not being too old or outdated; but you're always able to browse the archives and library for older artefacts. Anything breaking news, we send off immediately to our Notify subscribers – outside of this, the report covers the rest on a weekly basis.

So how does it all work? To view our methodology, sources and scoring matrix, head down to the appendices to get a feel for it all. Otherwise, information we deem as being 'key' is featured with insights and analysis supplied for reader's benefit. The rest of the information we pick up that can be categorised as security-based intelligence for DCU is placed thereafter. Our categorisation and tagging system mean that on a monthly basis, you'll get an overview of the statistics we've seen – updated in real-time, week-on-week for pattern recognition analysis.

1.2. FEATURED ADVISORIES (P2)

The prioritisation table and its dependencies are explained in Appendix A, and relate to how we filter, analyse and visualise the intelligence we collect.

Intrusion and Trespass	Priority
UK AAIB releases report on crash of DJI Matrice 600 due to GPS interference	**P2**

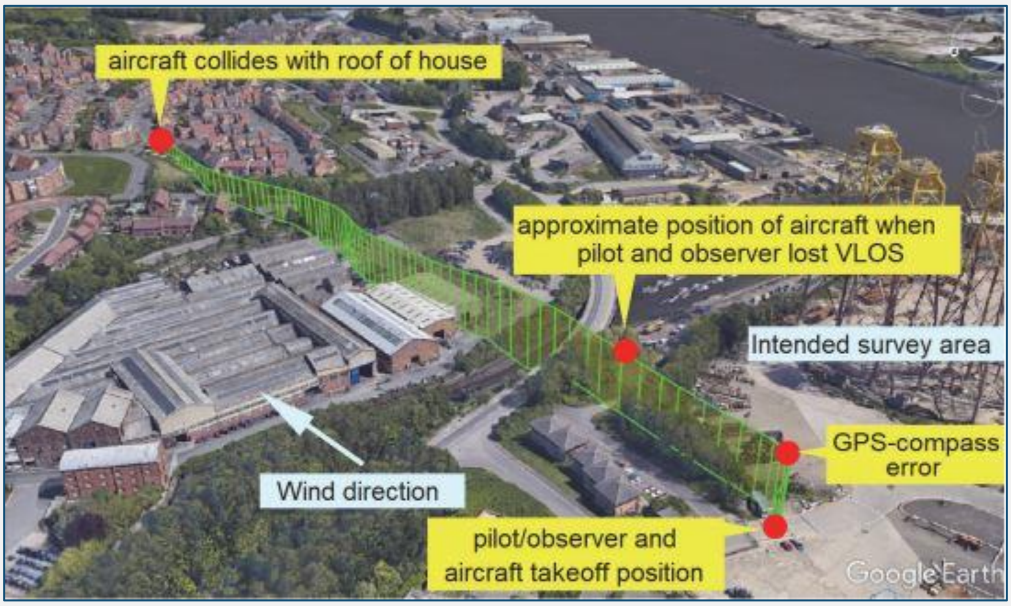
Summary

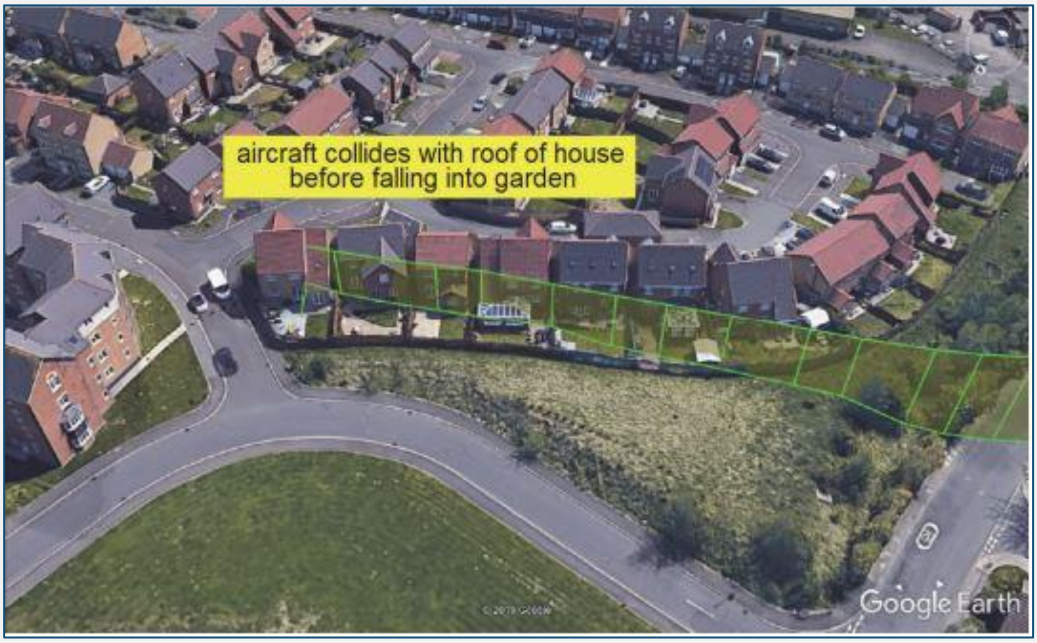
A DJI Matrice 600 used to survey a construction site experienced GPS-compass error and drifted out of the operator's line-of-sight before he could take over control of the drone. The drone crashed into a residential roof 300 meters away with no personnel injuries.

Overview

A DJI Matrice 600 Pro, under automated pre-programmed flight mode, was used commercially to survey a construction site with the pilot and drone registered officially with the UK aviation body. After completing three flights on 13 December 2019 at Wallsend, the operator was preparing for the last flight of the day with a near full charge of 97% battery power. During the take-off climb, the drone operator experienced an error message of "GPS-Compass Error" at 100 feet and observed that the drone stop its climb and remained stationary in the sky. However, the drone was slowly drifting north easterly towards the residential houses. The drone operator tried to engage "Return-To-Home" function several times, but the drone did not respond. Within ten seconds, the drone was out of visual range of the operator as it drifted past the line of trees along the boundaries of the construction site.

In the next minute, the drone flew across an industrial area and into the roof of a residential house 300 meters away before falling into the garden thereafter. There were no injuries to anyone during the incident. The local police were notified of the incident and the drone operator launched a second drone to look for the first one. However, the drone experienced a "Signal-Interference" error upon take off and the pilot immediately landed the drone. The drone was found by the owner of the house and handed it over to the police.


aircraft collides with roof of house
approximate position of aircraft when pilot and observer lost VLOS
Intended survey area
GPS-compass error
Wind direction
pilot/observer and aircraft takeoff position
Google Earth


aircraft collides with roof of house before falling into garden
Google Earth
©2019 Google

Analysis

Most drones operate on wireless frequencies, of which the channels and range can be shared by other devices. Although larger classes of drones that are mainly used in the military have their own protected channel to avoid 'sharing' with others, it is still possible for a loss of signal and communication link to occur. Interference can be caused by many reasons such as jamming or a malfunctioning hardware. However, in interference incidents like these, all commercial drones nowadays have a "Return Home" procedure which commands the aircraft to perform a series of actions such as returning and landing at its take-off point or flying to a marked location and spiralling downwards until it crash lands. In several older models, some drones might actually continue in their last commanded direction, instead of simply engaging the "Return Home" procedure – this is because the last command could be repeated continuously within the malfunctioning system, or the drone is within a looping pre-programmed flight.

In the Air Accidents Investigation Branch (AAIB) report, it was stated that the drone would engage "manual flight mode" when GPS or compass information is loss/mismatched. During normal autonomous flight modes, drones will aim to maintain its altitude and position by hovering on the spot with wings levelled using its in-built sensors. The sensors will help to counter environmental effects to keep the drone afloat at its pre-determined location. But in the DJI Matrice 600's manual flight mode, autonomous modes and the Return-To-

Home (RTH) mode (which is also an automated mode) would be disengaged and the drone operator is required to control the aircraft manually with the controller's joystick. When left stationary in this mode, the drone's suite of sensors, however, is not able to stabilise the drone's current location due to the lack of accurate GPS coordinates. This will result in the drone drifting in the direction of the wind. DJI has also verified that the manual flight mode was activate during this incident when there was a data mismatch between the GPS derived heading and the onboard magnetic compass heading.

In such an emergency, the operator will have to immediately take over control of the drone, or the drone will drift out of sight from the operator, possibly causing the drone to be out of range from the controller's command. AAIB reported that it only took 10 seconds before the drone went out of sight from the operator, a really short period of time. However, it is still possible for the operator to control the drone with the joystick, but in this incident, the operator was too focused on engaging the RTH mode that he did not attempt to input commands via the joysticks.

The drone operator is certified and is cognisant on the UK drone laws set in place by the UK Civil Aviation Authority (CAA), however, AAIB attributed the incident to a lack of familiarisation on handling such emergencies to the drone operator. Unlike pilots in the military where procedures and Bold Face Actions are routinely practiced to ensure familiarisation in times of emergencies, there are currently no requirements by the CAA to routinely practice on such emergencies or demonstrate on the operator's ability to navigate drones in a degraded flight mode for commercial drone activities. DroneSec agrees with AAIB's actions on having these safety measures recommended to the CAA as emergency handling skills are perishable and necessary to be maintained to prevent a risk of injury to people or damage to properties.

Recommendations

In the event something like this occurs, the crew should also have an incident response kit ready and waiting to collect the evidence, hardware and software data to piece together the story of what happened. Logging on both the drone, controllers and interconnected systems/software should provide enough telemetry data to discern what is accidental link-failure, bird strike or operator mistake over a malicious de-authentication attack, signal jam or protocol manipulation of the devices. In this incident, the drone operator informed the local police and activated his protocol on the use of a second drone to search for the first one. But as there was an ongoing signal interference, the response was marred and hindered. DroneSec recommends for the drone operator to review his incident response plan and to have a multi layered plan for such an occurrence.

DroneSec has always advocated for drone operators to keep themselves up to date and relevantly trained before operating a drone. It is recommended that drone operators have a good understanding on the capabilities of their drones – the intricate command functions available in the drone in every possible scenario, flight time, range and protocols or frequencies in use. Practicing on the worst-case scenarios and emergencies will hone the operator's familiarity on such events happening. These are important details which aid operators in planning their missions and handling ad-hoc changes when unexpected contingencies occur mid-flight.

Additionally, this incident is a clear example for aviation and communication authorities to regard the importance and impact of signal interference on drones. As drones operate on several wireless frequencies which are shared by other devices and services, certain measures must be taken to ensure that these frequencies do not get mixed into commercial uses. This could cause drones to experience signal disruption, resulting in incidents such as this one. The impact is greater in the future when urban air mobility or drone deliveries become a part and parcel of daily operations.

References

https://assets.publishing.service.gov.uk/media/5ee0dbb0e90e071424db3643/DJI_M600_Pro_UAS_reg_na_07-20.pdf

Notice to our readers: Featured advisories have provided context and field-based learnings to important incidents within the drone ecosystem. However, with the ever-growing database that we have, DroneSec has moved onto an online repository where artefacts and reports can be tracked, classified and analysed much easier.

Featured Analysis from now on are more comprehensive, wider in spectrum but only available on the Notify platform or to paid subscribers. If you would like continued featured summaries such as the above example, please get in touch with us or purchase a subscription.

Intrusion and Trespass	Priority
Israeli Defense Force hijacked and landed a Lebanese drone near border using CUAS	**P2**

[redacted]

1.3. NEWS AND EVENTS (P3)

455-passenger flight has near miss with illegal drone at Gatwick airport, United Kingdom

https://readsector.com/flight-with-455-passengers-came-within-300ft-of-hitting-drone-one-minute-after-taking-off/

Artsakh Defense Army shoots down Azerbaijani's Orbiter-3 surveillance drone

https://en.armradio.am/2020/07/18/artsakh-forces-down-azerbaijani-orbiter-3-drone/

Azerbaijani military shoots down two Armenian reconnaissance UAVs in Agdam and Tovuz

https://www.aa.com.tr/en/europe/azerbaijani-military-downs-2-armenian-drones/1917146

Special Monitoring Mission (SMM) UAV/mini-UAV experienced GPS signal interference in Ukraine by probable jamming near:

Ozarianivka, Zaitseve, Petrivka, Stepanivka, Kostiantynivka, Nelipivka, Andriivka, Pavlivske, Pleshchiivka and Orikhove on 16 July 2020

https://www.osce.org/files/2020-07-17%20Daily%20Report.pdf

Petrivske, Mykolaivka, Kostiantynivka, Mykhailivka, Romanivka, Novyi Svit, Korsun, Nyzhnie, Kadiivka, Stepanivka and Zolote on 18 July 2020

https://www.osce.org/files/2020-07-20%20SMM%20Daily%20Report.pdf

Zolote, Petrivske, Ivanopillia, Rozsadky, Kostiantynivka. Nyzhnie, Brianka, Khrestivka, Zorynsk, Brianka, Horlivka and Andriivka on 19 July 2020

https://www.osce.org/files/2020-07-20%20SMM%20Daily%20Report.pdf

Pyshchevyk and Lebedynske on 20 July 2020

https://www.osce.org/files/2020-07-21%20SMM%20Daily%20Report.pdf

Special Monitoring Mission (SMM) loses spatial control and mini-UAV by probable jamming in Ukraine near Chermalyk on 20 July 2020

https://www.osce.org/files/2020-07-21%20SMM%20Daily%20Report.pdf

Special Monitoring Mission (SMM) mini-UAV experienced being targeted and shot at in Ukraine near Petrivske on 19 July 2020

https://www.osce.org/files/2020-07-20%20SMM%20Daily%20Report.pdf

Special Monitoring Mission (SMM) mini-UAV experienced being targeted and shot at in Ukraine near Chermalyk, Pishchane on 20 July 2020

https://www.osce.org/files/2020-07-21%20SMM%20Daily%20Report.pdf

Reader Survey:
Are reports such as the Ukrainian Special Monitoring Mission reports useful? Please vote by clicking either: yes or no (you can close the page).

1.4. SOCIALS (P3)

Armenian Ministry of Defence displays list of Azerbaijani UAVs that were shot downed

https://twitter.com/301_AD/status/1285524435861110784

1.5. CYBER SECURITY (P3)

Parrot partners WISeKey for digital security solutions on ANAFI drones

https://blog.parrot.com/2020/07/15/wisekey-drone-security-partnership/

https://tdameritradenetwork.com/video/rB4AoXM8EVaBc1i9XsIH1w

1.6. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P4)

UK reviews launch of mobile police counter drone unit, to detect, track, identify and disrupt malicious drone activity. New ATMUA Bill to tackle drone misuse and enhanced powers.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/902593/HO_Annual_Report_and_Accounts_2019-20_FINAL.pdf (PDF Document - pg23)

USA Armed Services Committee to create a 'Counter Drone Center of Excellence' for rapid CUAS

https://docs.house.gov/billsthisweek/20200720/CRPT-116hrpt442.pdf (PDF Document - pg110)

ESAS proposes airworthiness standards for light UAS under 600kg

https://www.easa.europa.eu/sites/default/files/dfu/special_condition_light_uas.pdf

DroneResponders release guide for development and deployment of drones by first responders

https://www.droneresponders.org/the-five-cs

DJI recommends India's Civil Aviation Ministry to look at Remote ID instead of no permission no takeoff (NPNT) protocol (commentary)

https://www.medianama.com/2020/07/223-dji-drones-india-remote-identification/

Turkey, Israel and Iran have built some very lethal loitering munitions (commentary)

https://www.forbes.com/sites/pauliddon/2020/07/19/turkey-israel-and-iran-have-built-some-very-lethal-loitering-munitions/amp/?streamIndex=1

How are Israeli drones battling Chinese UAVs on India-China border (commentary)

https://eurasiantimes.com/india-china-battle-of-drones-how-israel-built-indian-drones-stack-up-against-chinese-uavs/

Drone Wars Open New Phase of Conflict In Syria (commentary)

https://www.zerohedge.com/markets/drone-wars-open-new-phase-conflict-syria

Hacking Drones – The UAV Digest (podcast)

http://theuavdigest.com/337-hacking-drones/

Operating in a Denied, Degraded and Disrupted Space Operational Environment (UAS)

https://ssilrc.army.mil/wp-content/uploads/2020/07/Conducting_Operations_in_a_Degraded_Space-Environment_18-28_Space_Operational_Environment1.pdf (PDF Document)

Neural-Swarm: Decentralized Close-Proximity Multirotor Control Using Learned Interactions

https://resolver.caltech.edu/CaltechAUTHORS:20191029-155055963 (PDF Document)

Agent Based Modelling for Low-cost Counter UAS Protocol in Prisons

https://search.proquest.com/openview/3c479c69e70a663bcb1cb10d83b6019c/1?pq-origsite=gscholar&cbl=4778292 (PDF Document)

Review of Counter-UAV Solutions Based on the Detection of Remote-Control Communication

https://ieeexplore.ieee.org/document/9142017 (PDF Available to Notify Customers in the platform)

1.7. SOCIALS (P3)

Armenian Ministry of Defence displays list of Azerbaijani UAVs that were shot downed

https://twitter.com/301_AD/status/1285524435861110784

1.8. COUNTER-DRONE SYSTEMS (P4)

US Army soldiers incorporate use of anti-drone guns as part of readiness training

https://defence-blog.com/news/army/u-s-army-soldiers-trains-to-take-down-drones.html

Leonardo DRS win USD $190m for development of Integrated UAS Defeat System

https://www.defense.gov/Newsroom/Contracts/Contract/Article/2280473//

Northrop Grumman incorporates Epirus' EMP system into CUAS to counter drone swarm threats

https://www.epirussystems.com/northrop-grumman-epirus-emp

Liteye Systems releases portable containerised counter drone system for US Air Force

https://liteye.com/liteye-c-auds-chosen-to-defend-critical-infrastructure-by-the-us-government/

Leidos announces a UAS Security Program Analyst role, supporting CUAS technologies

https://careers.leidos.com/jobs/5386975-uas-security-program-analyst-slash-planner

1.9. UTM SYSTEMS (P4)

Hanwha Systems partners Korea Airport Corporation for development of UAM technology

https://www.urbanairmobilitynews.com/business-partnerships/hanwha-systems-partners-with-airport-operator-in-new-uam-project/

In-Flight Data gets 1-year approval for BVLOS operations in Canada for public safety operations

https://globalnews.ca/news/7182510/okotoks-alberta-drone/

Terra Drone Indonesia approved for BVLOS surveillance and patrol operations in Indonesia

https://translate.google.com/translate?hl=en&sl=id&u=https://terra-drone.co.id/2020/07/17/press-release-terra-drone-indonesia/&prev=search&pto=aue

Droniq offers free usage of UTM system to encourage more BVLOS operations

https://www.unmannedairspace.info/latest-news-and-information/droniq-offers-short-term-free-utm-access-to-encourage-more-bvlos-operations/

Kenya Airways joins Global UTM Association for UTM development

https://www.facebook.com/KenyaAirwaysKE/photos/were-proud-to-join-the-global-utm-association-gutmaan-association-of-like-minded/10158021610593800/

Uber Elevate and Hidden Level collaborates to advance the safety of urban air mobility operations

https://hiddenlevel.com/press/hidden-level-uber-elevate-partnership/

1.10. INFORMATIONAL (P4)

Drones used by Delhi Police in thick jungle to locate bodies and solve double murder, India

https://timesofindia.indiatimes.com/city/delhi/delhi-police-use-drone-to-solve-double-murder/articleshow/77009863.cms

Golden Valley PD drones caught in privacy outrage from community after surveilling nudists

https://edition.cnn.com/2020/07/19/us/drones-nudity-minnesota-trnd/index.html

Indian-made Bharat drone to be used for India-China border surveillance

https://www.financialexpress.com/defence/drdo-provides-bharat-drones-to-indian-army-for-accurate-surveillance-at-india-china-border/2030882/

Russian Orlan-10 UAVs used for detection of adversaries' artilleries units for precision strike

https://www.armyrecognition.com/weapons_defence_industry_military_technology_uk/russian_army_uses_drones_to_detect_targets_for_howitzers_and_rocket_launchers_of_artillery_units.html

UK's 216 Squadron to trial drone swarms and Loyal Wingman onboard aircraft carriers

https://www.janes.com/defence-news/news-detail/raf-to-trial-unmanned-aircraft-from-royal-navy-carriers

UK Police face complaints on use of noisy helicopter, residents' favour use of drones instead

https://www.dailymail.co.uk/news/article-8537223/Police-face-growing-pressure-ground-noisy-helicopters-instead-use-drones-fight-crime.html

1.11. DRONE TECHNOLOGY (P5)

Boeing uses fighter jets to develop autonomous system for Australia's Loyal Wingman UAV

https://www.airlinenewsresource.com/boeing-continues-autonomous-flight-work-in-australian-outback-778.html

UK MoD procures UAVTEK's nano drone, Bug beating FLIR's Black Hornet 3 in tender

https://www.commercialdroneprofessional.com/mod-acquires-nano-drone-tech-with-uavtek-program/

FLIR Systems releases Hadron, a lightweight compact dual sensor camera system for drones

https://www.flir.com/news-center/camera-cores--components/flir-systems-announces-hadron-industrys-first-thermal-and-visible-sensor-module-for-drone-robotic-and-imaging-manufacturers/

University of Massachusetts Amherst awarded USD $750K grant to improve drone capabilities through edge and cloud computing

https://www.umass.edu/newsoffice/article/umass-amherst-led-research-team-receives

F-15 fighter jet spotted with Kratos UTAP-22 drone attached to its left underwing

https://www.thedrive.com/the-war-zone/34982/highly-modified-air-launched-loyal-wingman-drone-tested-with-air-force-f-15-eagle

Caltech researchers develops algorithm for close proximity drone swarm operations

https://www.caltech.edu/about/news/machine-learning-helps-robot-swarms-coordinate

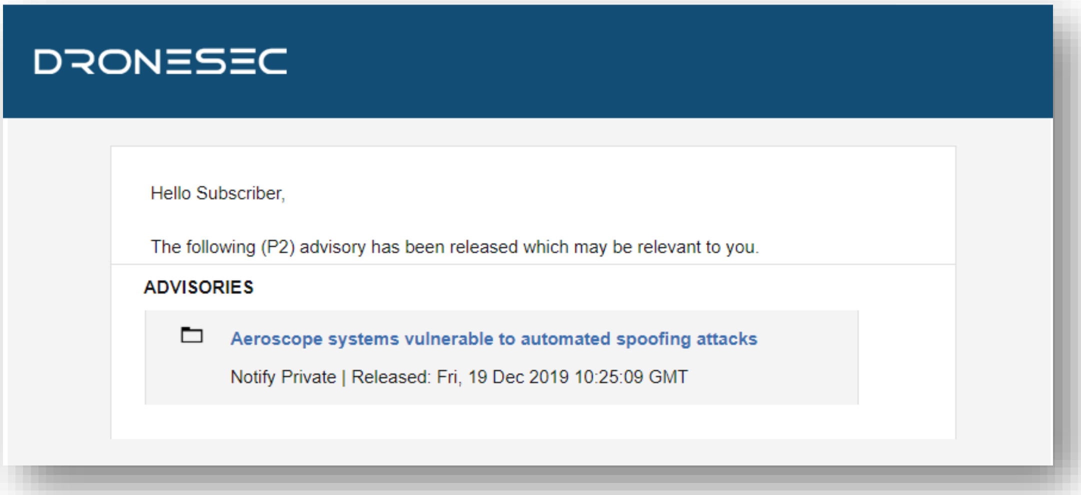
APPENDIX A: THREAT NOTIFICATION MATRIX

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.



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.