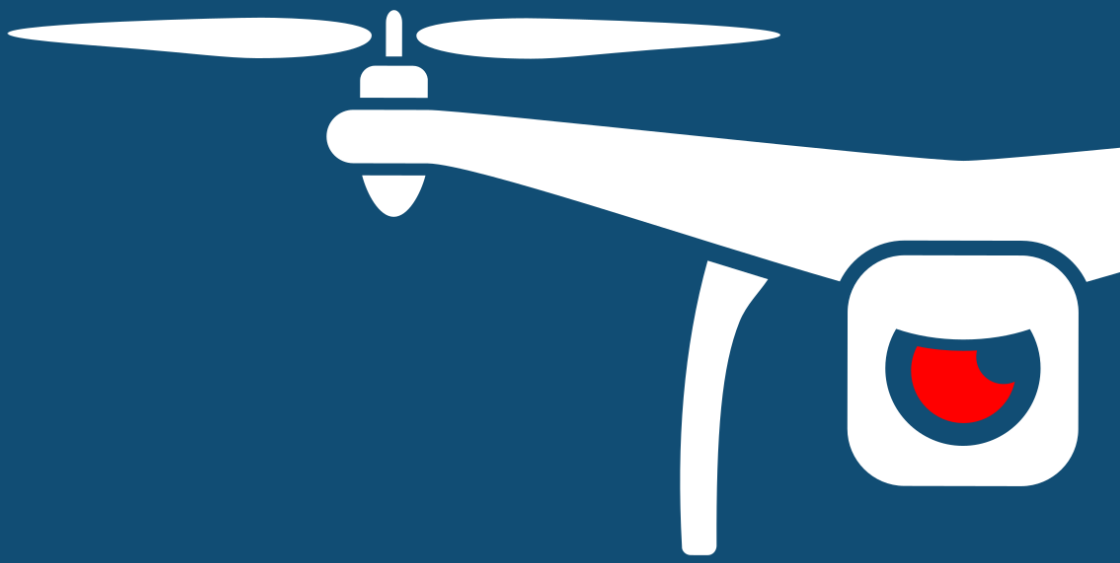
DRONE SEC
A Privasec COMPANY

NOTIFY ISSUE #57 (PUBLIC)

WEEKLY THREAT INTELLIGENCE

13 January 2021 | 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

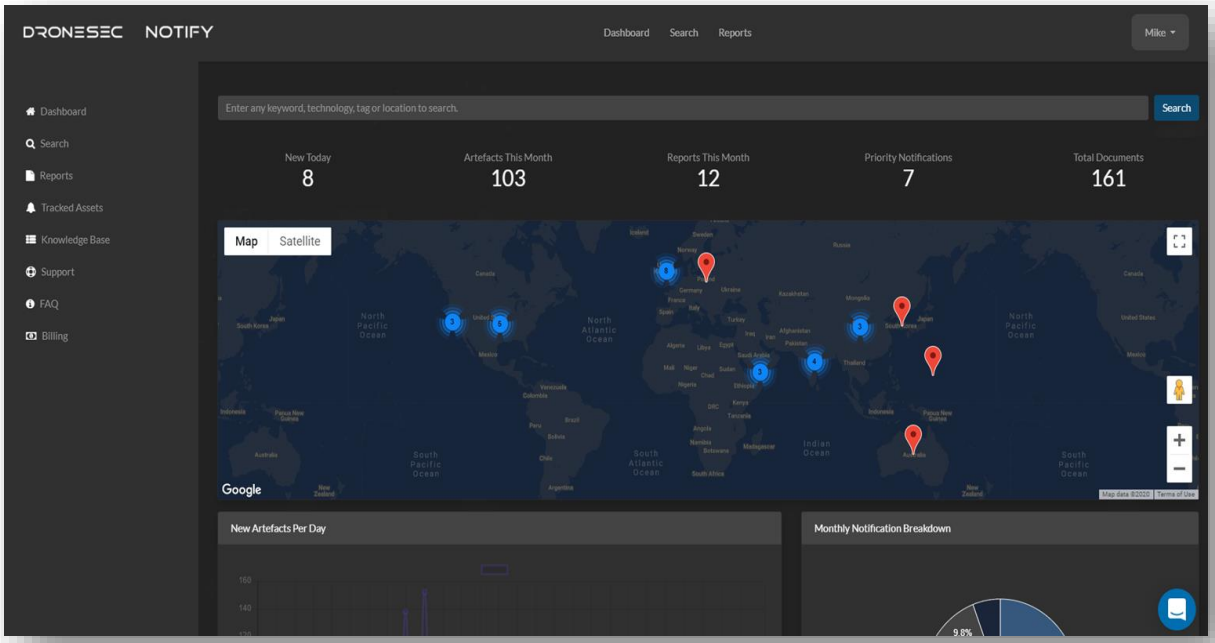
Email: info@dronesec.com

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

EXECUTIVE SUMMARY

New to Notify in 2021? This newsletter is a snippet of the information collected, triaged and categorised for statistical analysis in our Notify UAV Threat Intelligence Platform. Built from the ground up to record drone incidents, the platform creates a single operating picture for Law Enforcement and Governments world-wide to ascertain local, national and international threats posed by unmanned systems.

Notify aims to baseline the effectiveness of Counter-Drone strategies, systems and regulations. By harvesting the numerous signals, tactics, techniques and procedures of various threat actors utilising UAS for malicious activities, Notify can be harnessed by Red and Blue teams alike to accurately simulate and portray adversarial operations. Additional benefits include access to historical reports, a drone security program knowledge base and real-time keyword tracking and report notifications.



This week, we see the release of the US Department of Defense' Counter-Small Unmanned Aircraft Systems Strategy. Continuing in the US, the Army tested a number of drone detection systems in the dense, RF-heavy urban environment of New York City.

In general technology to watch, more details have emerged for Sony's new drone, and a patent released by technology giant Apple on drone communication technology (likely interfacing with Remote ID).

A number of prison deliveries continue to be recorded, and external analysis of a weaponised drone used by rebel militant groups in Syria is included.

As always, if you have comments or feedback, want to join in the discussion in our slack discussion group, or find the system that captures this information 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.

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

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
Man arrested for intent to deliver contraband with DJI Phantom 4 into Portlaoise Prison, Ireland	**P2**

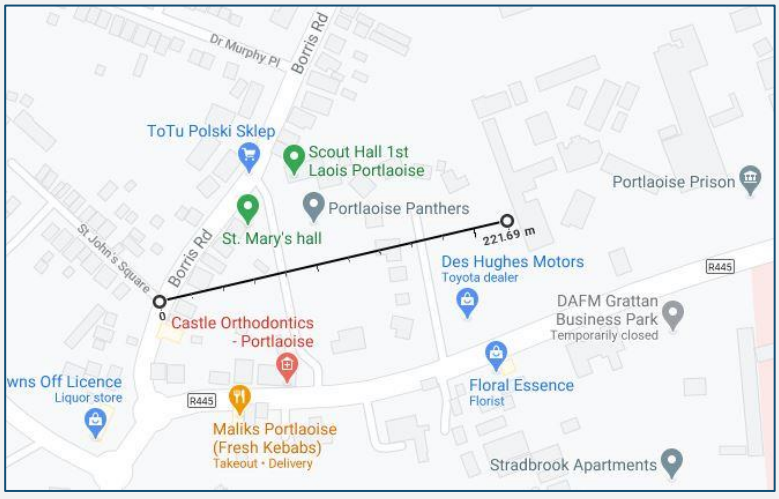
Summary

Irish Police arrested a man with a drone, narcotics and contraband with intent to deliver into a maximum security prison.

Overview

The Irish Police, Gardai, managed to foil a prison delivery attempt via a drone by closing in into an area where a gang was believed to have been trying to deliver contraband into Portlaoise Prison. Upon arrival, the Gardai managed to arrest a 20-year-old man, several contraband goods and spotted two cars which were suspected to have been used by the gang, however, the other gang members fled the scene. Contraband contained mobile phones, narcotics and phone chargers.

Although it was not stated how the Gardai came to know of the location, the arrest was made just in time as the gang and their drone was 230 meters from the prison perimeter.



Analysis

This incident reflects the growing number of gangs, criminal groups or even small time actors recognising the advantages of drones and utilising it to carry out illicit operations. Drones are an innovative solution against traditional methods of delivering contraband across restricted areas. Drones are easily available off the shelf for everyone and are known to reduce risk to the operators from being spotted and apprehended by law enforcement agencies as operators are located away from the immediate area of crime. Offenders for such contraband deliveries tend to get away easily as many secured or restricted facilities do not yet possess drone detection or counter-drone systems to mitigate the growing threat of drone intrusion.

However, with repeated incidents and case studies to learn from, federal agencies are proposing better counter drone laws to mitigate such threat. Similarly, law enforcement agencies are now more prepared against such acts and have measures in place against drone intrusions. Despite that, it can be still difficult to pinpoint the location of drone operators as they are located away from the immediate area of crime. These small sized drones can carry payloads of up to 5kg and can hover in the air for a long time at a high altitude, giving them an advantage to stay hidden until it is time to drop the payload.

However, the risk of being traced due to visual sighting or forensics exploitation on a downed/captured drone (via its video and photo footage) poses an exposure risk to the operators. Law enforcement officer can use this to their advantage and follow a drone to its operator in order to apprehend red-handed.

Threat Actor Group

Prison Drone Delivery Groups: https://help.dronesec.com/en/articles/4637701-prison-drone-delivery-groups

Recommendation

Drone operators are slowly mimicking these incidents that were prominent in United States, Canada and the United Kingdom in other countries around the world. Basic drone mitigation and preparation measures are recommended to respond to such incidents. Counter-drone systems that allow the detection of drones serve as a good step towards the prevention of drone deliveries. However, these systems are costly and partial purchases may not fulfill the criteria necessary for a full area protection.

A drone threat management Standard Operating Procedure (SOP) or incident response plan be drafted to govern the process, people and methodology in handling a drone, collecting evidence and responding to potential drone incidents. Agencies should start taking notice of aerial infringements and adjust their patrol timings and routes as these schedules could have already been recorded and logged by the criminal gangs or groups. Security agencies can undertake mock simulations and training scenarios in reacting to such rogue drone incidents to test and hone their response, improve communication flow between participating agencies, practice on the logging and monitoring of drone cases, mitigate risk and surface any challenges faced during the simulation.

Finally, enforcement agencies should appeal to the help of the public as an eyewitness or via their CCTV. Such information is beneficial as such evidence can lead to the discovery and arrest of persistent rogue drone operators.

References

https://www.irishtimes.com/news/crime-and-law/garda%C3%AD-foil-bid-to-fly-drugs-and-phones-into-portlaoise-prison-using-drone-1.4452687

Intrusion and Trespass	Priority
Drone operator arrested for trying to deliver mobile phones into HMP Perth, Scotland	**P2**

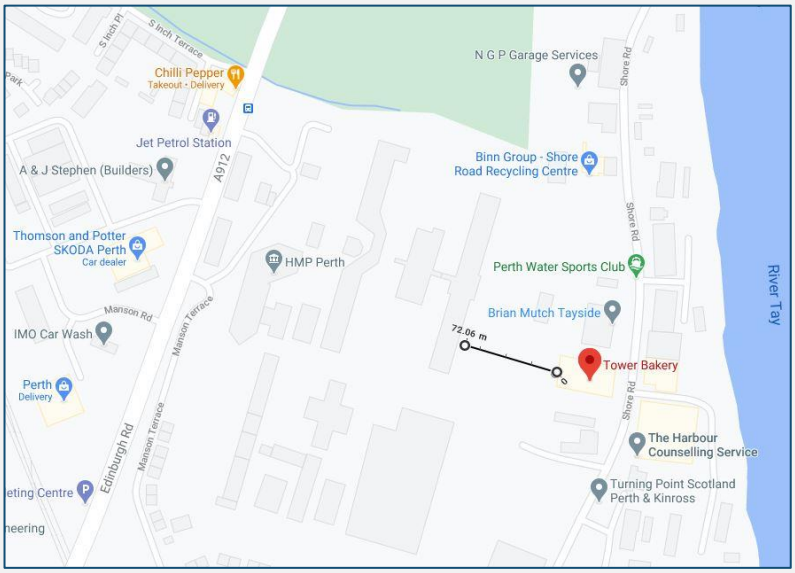
Summary

A man was offered a sum of money to ferry contraband into a prison via a drone. However, the operator crashed the drone and was subsequently arrested.

Overview

A man was offered by a client, whose boyfriend was in prison, to deliver contraband into HMP Perth, Scotland. After agreeing to the contract, the man flew his drone from behind a bakery, which was located about 80m from the prison cell blocks.

The man crashed his drone while trying to deliver mobile phones into the prison and was spotted by the prison security officers. The local law enforcement officers were alerted and the man was arrested soon after.



Analysis

This is a classic example of small time actors hinging on the benefits of drones to commit illegal acts. Drones are easily available with a low price point and the skill barrier to be able to fly a drone is not complex. Furthermore, drones can fly beyond visual line of sight (BVLOS) and carry payloads across vast distances. These factors make drones the tool of choice when it comes to delivery of contraband into a restricted area.

However, in order to reduce exposure, most of these nefarious drone operators tend to overload their drone or fly too quickly that they crash their drones into fixed installations. Law enforcement officers can seize these drones and perform forensics on the data stored within. Identification from the video footage or photographs can allow law enforcement to trace the starting and end points of the drone.

Threat Actor Group

Prison Drone Delivery Groups: https://help.dronesec.com/en/articles/4637701-prison-drone-delivery-groups

Recommendations

. A drone threat management Standard Operating Procedure (SOP) or Incident Response (IR) plan should be drafted to govern the process, people and methodology in responding and handling drones and the operators, collecting evidence and responding to potential drone incidents / drone operators in a pre-determined radius around the prison grounds. For example, security officers should start taking notice of aerial infringements and adjust their patrol timings and routes as these schedules could have already been surveilled and logged by the criminal gangs to avoid detection.

Security agencies can undertake mock or table-top simulations and training scenarios in reacting to such drone intrusions to test and hone their response, improve communication flow between participating agencies, practice on the logging and monitoring of drone cases, mitigate risk and surface any challenges faced during the simulation.

References

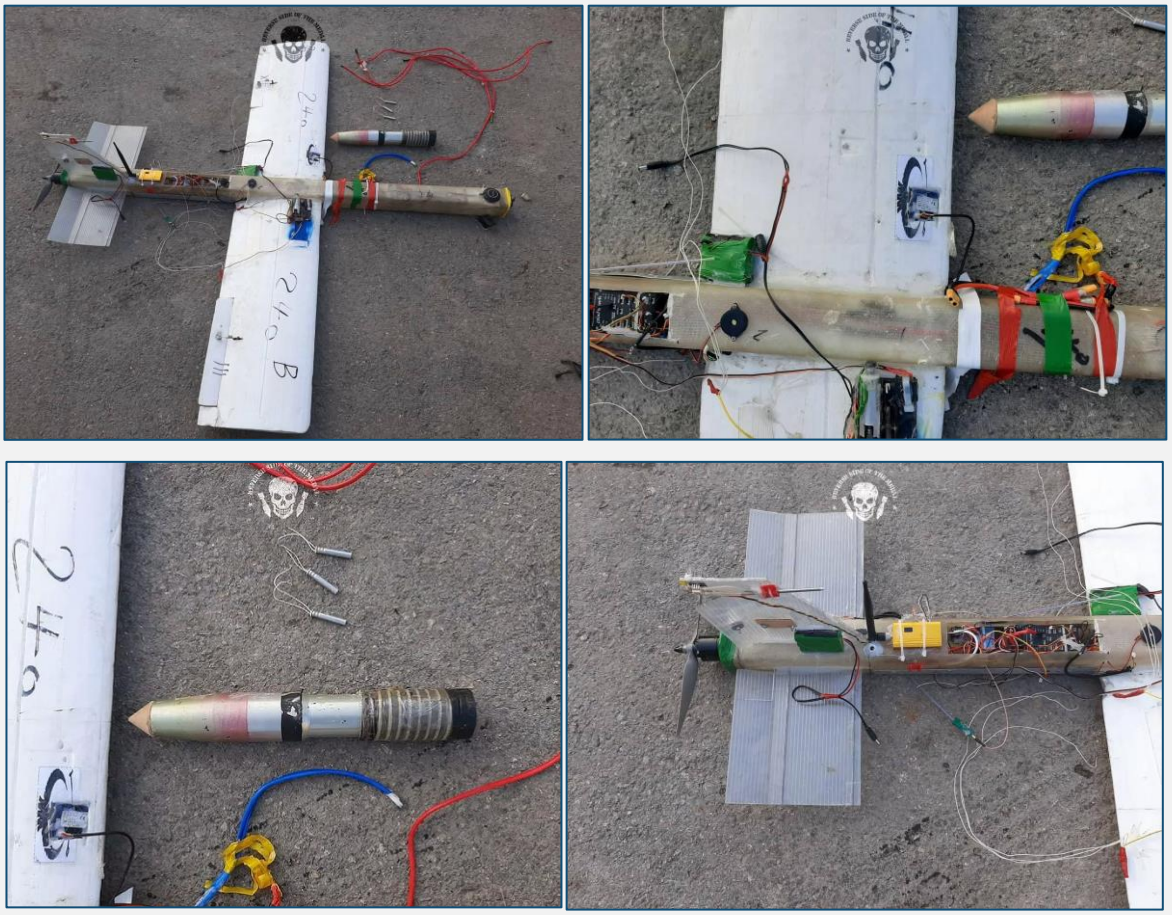
https://www.dailyrecord.co.uk/news/local-news/drone-pilot-jailed-six-months-23275991

Payloads and Custom Drones – External Analysis	Priority
Homemade Rebel Weaponised Drone Analysed	**P2**

Overview

A homemade rebel drone was shot down by the Syrian Army in December 2020 via electronic countermeasures. An external source has provided the analysis of the drone within the [DroneSec Slack Discussion Group] and was open to sharing the information with Notify readers.

Analysis



Component Analysis

Controller appears to be a Pixhawk 4. The use of Pixhawk components was to be expected. PX4 items can be easily obtained online. For example, the "PX4 Differential Airspeed Pitot Tube" and "Pitot Tube Air speedometer Airspeed Sensor" for Pixhawk 4 flight controller can be found available easily on AliExpress: https://de.aliexpress.com/item/32756505477.html

- Drive with electric motor - a short range under 10 km. Unfortunately, the batteries are already removed - otherwise we could analyse more about the capacity.
- In the front of the tip are both GPS and possibly a camera built in (the camera angle for the tip of the drone is not clear, hence why possibly).
- The drone has about 1m length and about 1m wingspan.
- The receiver is hard to identify through the packaging, but from the antenna it could be a long-range receiver with more than 10km range.
- The size of the explosive charge is not easy to determine - but should be about 100 to 200 grams given the size. The effect is allowed to be comparable with a hand grenade.

- So fortunately, this is not yet a fully autonomous drone (which would be possible with the technology) and target approach is probably via GPS and camera. Therefore, taking it down via electronic warfare was still possible.
- Material costs: less than $700 USD

Further Analysis on Payload Weight Capacity

Via estimation, the wingspan is about 1m and the length of each wing about 25cm. The wing area is assumed to be 25 dm2. The air foil is unknown. With this size, a wing loading of perhaps 100grams / dm2 is reasonable (also depends on the power of the motor and the speed). This would give us a take-off weight of 2 to 2.5 kilograms.

Using weight data from: https://www.instructables.com/Design-Build-Your-Own-Electric-RC-Airplane/

- 1x motor =80g
- 1x 2200mAh Batteries = 200g
- 2x ESC = 35g
- 6x servos 25g each x6 = 150g
- 1x BEC = 35g
- 1x Receiver = 15g
- Total = 515g
- Margin for aircraft weight: 515g * 2.5 = 1287.5g
- Wing loading calculated back: 1287.5g / 25 dm2 = 51.5g/dm2

We now have calculated possible values between 1300g and 2500g. Since this is technically rather an unclean design with poor aerodynamics and little space, the payload will be rather in the lower range. I would assume an upper limit of about 200 to 300g of explosives. This makes it primarily a weapon against soft targets.

However, with a well-designed model, I would also consider 1 kg payload possible. This is only a very rough estimate because key parameters are unknown. However, with 300g of explosives you can do a lot of damage - especially if the pilot can target specific targets.

References

https://www.instagram.com/p/CJ04_qDr92G/?igshid=81ov7kzya16j

https://www.linkedin.com/in/ulf-barth/

1.3. NEWS AND EVENTS (P3)

Drone sighting closes Christchurch Airport for 15 minutes, New Zealand

https://www.stuff.co.nz/national/123796176/drone-forces-temporary-closure-of-christchurch-airport

Yemeni military destroys explosive-laden drone near Aden's presidential Maasheeq Palace

https://english.alarabiya.net/en/News/gulf/2020/12/30/Yemeni-military-intercepts-explosive-laden-drone-near-Aden-s-presidential-palace

Drone strikes oil refineries in Aleppo, Syria

https://www.syriahr.com/en/199747/

Drone found crashed near Chepstow racecourse

https://www.dailymail.co.uk/sport/racing/article-9135905/Police-launch-probe-drone-crashes-near-Chepstow-racecourse-Welsh-Grand-National-meeting.html

Four arrested after failed attempt to deliver drugs via drone into a prison in Sherbrooke

https://montreal.ctvnews.ca/four-arrested-in-attempt-to-deliver-drugs-to-sherbrooke-prison-with-drone-1.5262827

Singaporean man charged for flying near Singapore-Malaysia border check point without permit

https://www.tnp.sg/news/singapore/man-be-charged-over-flying-drone-near-woodlands-checkpoint

Residents report drug smuggling drone activities around San Diego neighbourhoods

https://fox5sandiego.com/news/border-report/drug-smuggling-drones-soaring-over-border-into-residential-neighborhoods-agents-say/

1.4. CYBER AND DATA SECURITY (P3)

Why internet-based tracking of drones is less of a privacy concern than a RF-based one (commentary)

https://www.theverge.com/2021/1/1/22209558/google-wing-faa-drone-remote-id-broadcast-rule-privacy-security

Kittyhawk highlights existing unsolved issues despite FAA's Remote ID regulation for drones (commentary)

https://kittyhawk.io/blog/remote-identification-of-drones-were-there/

1.5. SOCIALS (P3)

Alleged police drone attacked with fireworks in Timaru, New Zealand

https://www.tiktok.com/@teamhategrip/video/6895587305839414529?lang=en (*language warning*)

Taliban insurgents filmed flying and training on drones, Afghanistan

https://twitter.com/KabirTaneja/status/1348472028089655296

Forums discusses feasibility of modding DJI Mini 2 to include goggles and OcuSync

https://mavicpilots.com/threads/ocusync-2-0-with-goggle-hacks.104835/

Chinese CETC showcases air launched loitering drone swarm

https://www.youtube.com/watch?v=QamGaDNczJw

1.6. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P3)

US DoD releases Counter-Small Unmanned Aircraft Systems Strategy

https://www.defensenews.com/pentagon/2021/01/07/joint-strategy-calls-for-common-architecture-to-counter-increasingly-complex-drone-threats/

https://media.defense.gov/2021/Jan/07/2002561080/-1/-1/1/DEPARTMENT-OF-DEFENSE-COUNTER-SMALL-UNMANNED-AIRCRAFT-SYSTEMS-STRATEGY.PDF (PDF Document)

ICAO introduces model drone regulatory framework as a guide for drone operations

https://www.icao.int/safety/UA/Pages/ICAO-Model-UAS-Regulations.aspx

Netherlands introduces new drone laws, effective December 31, 2020

https://zoek.officielebekendmakingen.nl/stcrt-2020-66578.html#d17e867

China's first national standard for drone deliveries to begin on January 1, 2021

http://www.spb.gov.cn/zc/ghjbz_1/201508/W020201204542195544172.pdf (PDF Document)

FAA bans drones around two DoD facilities citing past security-sensitive drone activity

https://qctimes.com/business/faa-bans-drones-over-the-rock-island-arsenal/article_0606e467-b643-5cb3-8b53-9a3515af0c04.html

Security, protracted conflicts and the role of drones in Eurasia

https://dronewars.net/wp-content/uploads/2021/01/DW-Eurasia-WEB.pdf

U.S. Military Bases: Could a drone swarm attack mean doom? (commentary)

https://nationalinterest.org/blog/buzz/us-military-bases-could-drone-swarm-attack-mean-doom-176122

Uncle Sam Needs AI, ASAP: DoD Artificial Intelligence Chief (commentary)

https://breakingdefense.com/2021/01/uncle-sam-needs-ai-asap-dod-artificial-intelligence-chief/

Strategic Imperatives Shaping the C-sUAS Industry in 2021 (commentary)

https://medium.com/@pain.management/strategic-imperatives-shaping-the-c-suas-industry-in-2021-179db3d95477

Aerial-Ground Interference Mitigation for Cellular-Connected UAV

https://arxiv.org/pdf/2101.01859.pdf

The State of Cybersecurity in UAV Used in Critical Infrastructure

(PDF Document: Available within the Notify Platform)

1.7. COUNTER-DRONE SYSTEMS (P4)

US Army tests drone detection systems on rooftops of dense urban environment, New York City

https://www.army.mil/article/242163

Counter drone technologies face slow ramp-up at airports globally (commentary)

https://www.wsj.com/articles/counterdrone-technologies-face-slow-ramp-up-at-airports-globally-11546283774

Rafael upgrades Drone Dome to intercept drone swarms

https://www.unmannedairspace.info/counter-uas-systems-and-policies/drome-dome-c-uas-upgraded-to-defend-against-drone-swarms/

Dubai Cusp Technologies uses magnetic beams to repel hostile drone attacks

https://gulfnews.com/business/company-releases/dubai-tech-firm-develops-magnetic-shield-to-counter-drone-attacks-1.1609665770046

1.8. UTM SYSTEMS (P4)

Apple patents drone communications technology

https://dronelife.com/2021/01/11/apple-patent-for-drone-communications-technology-is-apple-getting-into-the-industry/

Escribano contracted to develop for multiplatform drone swarm system for Spanish Army

https://defence-blog.com/news/army/spanish-army-awards-contract-to-escribano-for-multiplatform-swarm-system.html

Thales, Telstra and Geelong City to develop a Low Altitude Airspace Management system

https://www.unmannedairspace.info/latest-news-and-information/thales-telstra-and-geelong-city-develop-low-altitude-airspace-management-system/

United Kingdom and Scotland invest £5.6Mil to develop drone airspace at Montrose Drone Port

https://www.unmannedairspace.info/latest-news-and-information/scottish-drone-port-receives-gbp5-6-million-government-grant-to-establish-offshore-trial-airspace/

Red Cat partners Skypersonic to complete remote drone flight 1200 miles away

https://www.suasnews.com/2021/01/red-cat-partners-with-skypersonic-completes-long-distance-drone-flight-remotely/

1.9. INFORMATIONAL (P5)

Parrot contracted to supply ANAFI drones to French army

https://www.lemonde.fr/economie/article/2021/01/11/l-armee-francaise-fera-voler-des-drones-parrot_6065910_3234.html

Drones instrumental in assisting fights against fire, Fargo Fire Department

https://www.grandforksherald.com/news/fires/6822024-Drones-instrumental-in-helping-crews-fight-major-Fargo-fire

Woodbury PD to purchase DJI Matrice 300 RTK to enhance search and rescue capabilities

https://www.startribune.com/woodbury-to-join-cities-flying-drones/600005704/

Port St. Lucie PD utilise DJI Mavic 2 drone to find missing children

https://dronedj.com/2021/01/06/florida-police-use-a-drone-to-help-locate-two-missing-children/

Teenager rescues four drowning fishermen out in the Arabian sea with help of drone, India

https://www.hindustantimes.com/india-news/armed-with-drone-19-year-old-rescues-4-drowning-fishermen-off-kerala-coast/story-nvCNgclVlaxfuuG4Q4HuPP.html

Connecticut PD deploys drones to search for armed suspect

https://www.myrecordjournal.com/News/State/Police-use-dogs-drones-in-search-for-shooting-suspect.html

Rutherford County PD utilised drone to search for lost woman in wooded area

https://www.newschannel5.com/news/emergency-response-teams-use-drones-to-find-missing-rutherford-co-woman

1.10. DRONE TECHNOLOGY (P5)

Baykar Defense develops SATCOM variant for TB2, TB2S, accomplishes first test flight

https://www.uasvision.com/2021/01/08/satcom-integrated-bayraktar-tb2s-performs-first-flight/

Huawei reveals patent on drone control system and methodology

https://www.gizmochina.com/2021/01/06/huawei-drone-control-system-patent/

Israel focuses on developing drone technologies that supports GPS-denied environments

https://www.unmannedairspace.info/latest-news-and-information/israel-developing-new-drone-communication-technologies-following-gps-signal-disruptions/

Engineers design mechanical gripper to allow drones to hang from objects, save battery power

https://newatlas.com/drones/mechanical-gripper-drones-perch/

Sony reveals Airpeak drone with a7S III camera as sensor payload

https://www.youtube.com/watch?v=6kxqEkpMi5M

General Atomics selected to support Skyborg with its Avenger jet-powered drone

https://www.ga-asi.com/ga-asi-selected-for-skyborg-vanguard-program

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.

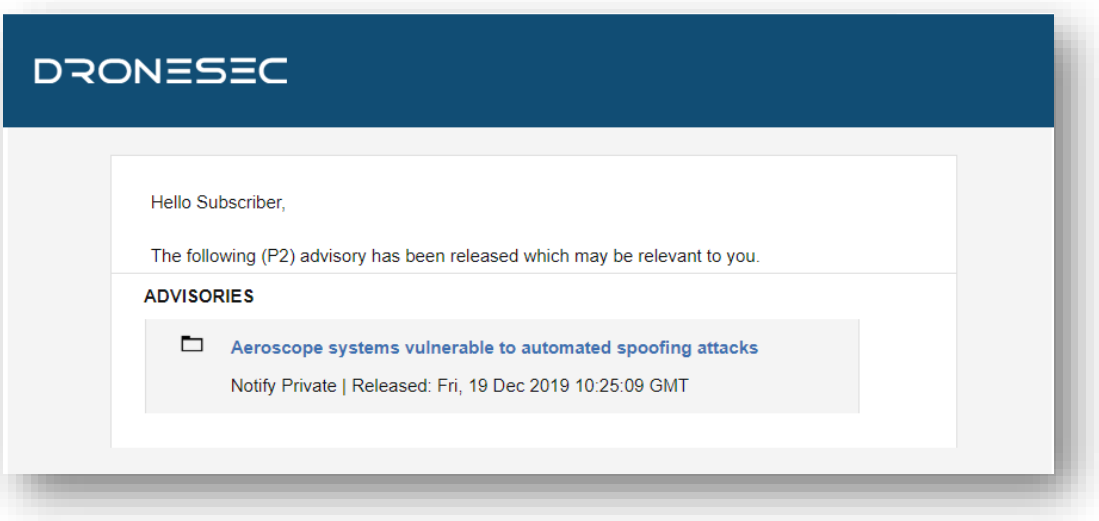


Figure 1 - A threat notification specific to a Notify customer's listed keywords.

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.