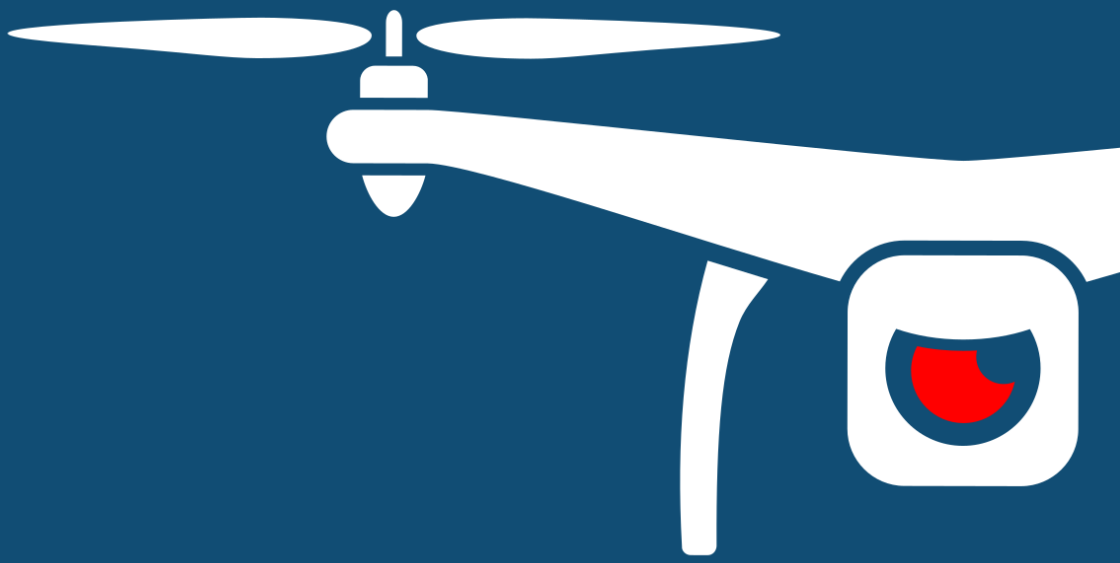
DRONE SEC
A Privasec COMPANY

NOTIFY ISSUE #18

WEEKLY THREAT INTELLIGENCE

15 April 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

Another interesting week with drone incidents around Correctional Facilities that are resulting in more arrests; previously, many operators were managing to get away with simple contraband delivery. The problem is still mostly understated however, with many prisons not realising the impact they may have had without realising.

This week the office of the Attorney General of USA released their guidance on protecting facilities and assets from drones, which has sparked a large amount of healthy debate – a few key questions have arisen too, such as the influx of Police Departments utilising drones for surveillance operations and the legalities around it. In a similar context, ACLU has sued Baltimore Police Department over their surveillance program and Idaho has passed laws removing the need for LE and Emergency services requiring a warrant when executing drone operations in critical events.

We've included a DIY-style reverse engineering post of the Potensic d85 drone's wireless protocol and the DJI RM500. The Australian Army has set up "RICO" – a specialist department focusing on unmanned systems and the opportunities they provide.

On a personal note, we're now entering our sixth week here in lockdown. It is a tough time for all and we're conscious of the mental strain it can take on both business owners and employees. If you'd like to chat, discuss anything drone security or just say hello, feel free to join our slack channel.

- *Mike Monnik, DroneSec CTO*

TABLE OF **CONTENTS**

1. Threat intelligence ---- 5
1.1. Introduction ---- 5
1.2. Featured Advisories (P2) ---- 6
1.3. News and Events (P3) ---- 8
1.4. Socials (P3) ---- 9
1.5. Whitepapers, Publications & Regulations (P3) ---- 9
1.6. UTM Systems (P4) ---- 9
1.7. Informational (P5) ---- 10
1.8. Drone Technology (P5) ---- 10
APPENDIX A: Threat Notification Matrix ---- 12
A.1. Objectives ---- 12
APPENDIX B: Sources & Limitations ---- 16
B.1. Intelligence sources ---- 16
B.2. Limitations ---- 17

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
Drone located within tree near Collins Bay Institution perimeter	Drones, Illegal Infringement, Prison, Security	P2

Summary

A drone suspected for making contraband delivery was found in a tree near the institution.

Overview

An officer from the Kingston Police noticed a drone stuck in a tree near Collins Bay Institution, Canada, and activated the Penitentiary Squad for the removal of the drone. Further investigation shown that the drone was on its way back from the Institution, however, the drone was not carrying any payload. The drone operator has not been caught and the investigation is still ongoing.

Analysis

The location of the Institution and where the drone was found was roughly 1 kilometre apart. This distance is well within the flying range and time for most COTS drones allowing rogue operators to send contraband to inmates behind secured and restricted areas. In most of these cases offenders deliberately avoid registering their drones to avoid detection by law enforcement, reducing the possibility of apprehension. Furthermore, the skill barrier to be able to fly a drone is not complex. 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.

Recommendation

All restricted and secured areas should have a Drone Security Management Plan in place to deal with small unmanned systems. 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.

While it was unclear if Collins Bay Institution had this SOP in place, they called several agencies for the retrieval and management of the drone incident. DroneSec recommends that such incidents should be logged and categorised appropriately baselined by a drone-incident form. 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. This information can aid enforcement agencies 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. Similarly, correctional facilities should undertake mock simulations in reacting to both in-air and downed drones to hone their response, improve communication flow between agencies and monitor repeated progress.

References

- https://www.kingstonist.com/news/drone-snagged-in-tree-near-collins-bay-institution/

Security	Tags	Priority
Three arrested for attempted delivery into Hays State Prison	Drones, Illegal Infringement, Prison, Contraband, Security	P2

Summary

Three individuals were caught before the act was committed with alleged intent to deliver drugs and a cellular device into the prison via a drone.

Overview

Three individuals were arrested after they were caught possessing drugs and synthetic drugs with an intent to deliver to an inmate at the Hays State Prison in the US. The three individuals admitted that they were planning to use a drone to send tobacco, drugs and a cellular device across the walls into the prison. However, the group were caught on a highway before the act was carried out. Further information was not available as the investigation is still ongoing.

References

- https://coosavalleynews.com/2020/04/suspects-to-use-drone-to-give-prison-inmate-tobacco-and-phone/

Security	Tags	Priority
Man arrested for attempted delivery into Erlestoke Prison	Drones, Illegal Infringement, Prison, Contraband, Security	P2

Summary

Police arrested a man on suspicion of attempting to smuggle contraband inside Erlestoke Prison.

Overview

A 30-year-old man from Southampton, UK, was taken into custody after his drone was spotted trying to drop a package inside the prison fence perimiter. Prison officers spotted the drone and immediately traced it to the operator who was hiding in a wooded area near the prison. The package was classified as a List A item which included drugs, explosives, firearms and ammunitions. No further information such as drone model has been provided as investigation is still ongoing.

References

- https://www.thisiswiltshire.co.uk/news/18370023.police-question-man-alleged-attempt-smuggle-class-substances/

Security	Tags	Priority
DJI RM500 smart controller rooted	Drones, Security, Attack Vector	P2

Summary

A member of an internet forum managed to root (unlock and bypass restrictions) the DJI RM500 smart controller, allowing them to boost the signal strength to their drone.

Overview

Amstar, a member of the Mavic Pilots forum, found a way to root the DJI smart controller via the use of third-party software. Doing so allowed him to boost the signal strength of his drone, flying it an additional 2 miles

further than before. The member also mentioned that several features in the drone was 'locked' and rooting the controller allowed him to unlock these features and enhanced the capabilities of his drone.

Analysis

Modding DJI equipment is not new, and in some cases has a commercial incentive; in the past, popular Russian modding forum nolimitdronez.com has offered bounty payments in return for mods. Not all these mods are harmless fun however – if used by malicious individuals, these may play out in a similar fashion to the exchange of paid vulnerabilities or exploits as seen in cyber security.

While rooting the smart controller allows operators to 'enhance' their drones, it actively voids the warranty of the drone and cause the drone to operate in a possibly unsafe environment. Enhancements made to the drones may have been disabled on purpose by the manufacturer due to its instability, inability to sustain such operations or interference of active communication frequencies. Operators may not know the consequences of such modifications. It could result in a significantly lower battery life, or an emission of frequencies which could affect and shut out other devices.

References

- https://mavicpilots.com/threads/successful-rooting-of-rm500-also-known-as-the-smart-controller.62580/ (contribution by Notify member)

1.3. NEWS AND EVENTS (P3)

Indian Army Mavic 2 quadcopter shot down after flying 600m into Pakistani airspace

https://www.straitstimes.com/asia/south-asia/pakistan-shoots-down-indian-drone-as-kashmir-tensions-rise

ACLU sues Baltimore Police Department, USA, over aerial surveillance program

https://www.theroot.com/aclu-sues-baltimore-police-department-over-aerial-surve-1842819613

Australian Army sets up specialist office RICO to advance knowledge in unmanned systems

https://www.defenceconnect.com.au/land-amphibious/5873-army-sets-up-rico-office-for-robotic-and-autonomous-systems/amp

Drones deployed to search for escaped inmates from Correctional Center in McAlester, USA

https://www.mcalesternews.com/covid-19/update-drone-dogs-plane-being-used-in-search-for-latest-escaped-inmate/article_8d0349aa-7a6a-11ea-8151-73cc3f562d64.html

NY anti-COVID broadcast drone operator identified as youtuber 'droneXfactor' (UPDATE)

https://www.youtube.com/watch?v=aDBmCxa_iz0&feature=youtu.be&t=27 (contribution by Notify member)

US Army Research Lab studies into drones that can be launched from a grenade launcher

https://www.army.mil/article/234300/grenade_launchers_able_to_fire_armys_new_camera_drones

Barodian Police, India request citizens to help enforce lockdown with personal drones after arresting 66 people with department-owned drones

https://timesofindia.indiatimes.com/city/vadodara/help-us-with-your-drones-cops-urge-barodians/articleshow/75088727.cms

Forensic Crash Unit, QLD Police in Australia carry drones on motorcycles

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

1.4. SOCIALS (P3)

Reverse Engineering a Potensic d85 drone's wireless protocol

https://www.reddit.com/r/hacking/comments/fy5pi2/is_hardware_hackingreverse_engineering_allowed/

https://github.com/enp2s0/d85decode

Assessing the FCC hack for the Mavic Mini (opinion)

https://www.youtube.com/watch?v=hXjr8DXxMp4

1.5. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P3)

US Attorney General releases guidance on protecting facilities and assets from drones

https://www.defensedaily.com/barr-issues-guidance-enabling-justice-department-exercise-counter-drone-authorities/unmanned-systems/

https://www.justice.gov/ag/page/file/1268401/download (PDF)

Kenya, Africa, Civil Aviation approves drone operations with laws in place

https://www.kcaa.or.ke/sites/default/files/publication/Draft_CiviAviation_Unmanned_Aircraft_Systems_Regulations_2019_Revised.pdf (PDF file)

Idaho legislation allows LE and emergency services to use drones without a warrant

https://www.ktvb.com/article/news/local/capitol-watch/drones-idaho-lawmaker-bill-additional-restrictions/277-71ae242e-e5e2-4ef7-852b-3a3477d935e7

Exploiting multi-vendor vulnerabilities as back-doors to counter the threat of rogue small unmanned aerial systems

https://www.mendeley.com/catalogue/17d9d9d0-8acd-3b75-8bbb-f88231957b53/ (PDF available to Notify customers)

How to detect cyber-attacks in unmanned aerial vehicles network

https://www.mendeley.com/catalogue/a2cef4de-faac-3663-bf57-651592d673c3/ (PDF available to Notify customers)

Unmanned aerial vehicle (drone) usage in the 21st century – loss and crime prevention

https://www.sciencedirect.com/science/article/pii/B9780128172735000144 (PDF available to Notify customers)

1.6. UTM SYSTEMS (P4)

FAA selects Virginia Tech Aviation Partnership and Griffiss International Airport as test site participants for Phase 2 of UTM Pilot Program (UPP)

https://www.faa.gov/news/updates/?newsId=95371

Iris Automation launches 360-degree detect-and-avoid system for BVLOS drone flight

https://www.irisonboard.com/2020/04/06/press-release-iris-automation-announces-casia-360/

FAA awards $2.6 million in grants for UAS research, education and training to universities

https://www.faa.gov/news/press_releases/news_story.cfm?newsId=24799

US Considers how to open skies to drones and flying unmanned vehicles (OPINION)

https://www.ft.com/content/a0341b02-54cd-11ea-8841-482eed0038b1?sharetype=blocked

1.7. INFORMATIONAL (P5)

Interference between unlicensed frequencies of Wi-Fi and drones (Commentary)

https://it.toolbox.com/blogs/leebadman/wi-fi-and-drones-can-ruin-each-others-day-041320

Downed drone confiscated in Dearborn Michigan, USA

https://www.thenewsherald.com/news/state/drone-confiscated-near-woman-s-bedroom-window/article_d6d8dab9-8059-5ffa-98fa-c6b419d06385.html

Promark Warrior drone located in backyard in Arizona, USA

https://www.nogalesinternational.com/news/drone-was-unexpected-find-in-local-woman-s-backyard/article_9c704a8e-7dc4-11ea-88d8-cf51d355c495.html

Legal and safety rules for drone flights in South Africa (Commentary)

https://www.linkedin.com/pulse/where-can-i-fly-my-drone-kim-james/

Lincolnshire Police deploys drone with thermal imaging to find missing vulnerable man sitting on train tracks

https://www.lincolnshirelive.co.uk/news/local-news/police-drone-missing-person-railway-4039889

1.8. DRONE TECHNOLOGY (P5)

Volocopter's passenger drone now carries 200kg payload with spray technology

https://www.producer.com/2020/04/spray-drone-with-payloads-up-to-200-kg/

Digital Aerolus 120-UVC develops indoor GPS-free drone disinfects with C-band UV light

https://digitalaerolus.com/aertos-120-uvc-drone-disinfection-essential-businesses/

Lewes PD, USA, to deploy drone as part of virus lockdown tactic

https://delawarestatenews.net/coronavirus/lewes-pd-drone-part-of-tactics-to-curb-virus-spread/

Mysuru, India, deploys ideaForge drones to enforce lockdown due to citizens' non-compliance

https://www.business-standard.com/article/current-affairs/dumping-old-ways-in-lockdown-mysuru-city-uses-drones-for-announcement-120040901553_1.html

Kotwali Police, Bangladesh, uses Mavic 2 drone to enforce social distancing

https://en.prothomalo.com/bangladesh/cmp-using-drones-to-ensure-social-distancing

Treviolo Police, Italy, equips Mavic 2 with thermal sensor for temperature screening

https://www.thelocal.it/20200410/hovering-police-drones-take-italians-temperature-and-issue-fines

Honolulu Fire Department deploys three drone team with Mavic 2 to enforce beach lockdown

https://www.kitv.com/story/41996004/drones-to-assist-in-enforcement-of-stay-at-home-order

Gomtipur police, India, trials drone for medicine delivery

https://timesofindia.indiatimes.com/city/ahmedabad/gomtipur-police-use-drone-to-deliver-medicines/articleshow/75130729.cms

Meriden Police Department, US, utilising a Mavic 2 drone for monitoring social distancing

https://www.nbcconnecticut.com/news/local/meriden-police-to-use-drone-to-monitor-parks-trails/2255104/

Savannah PD deploys two of five Mavic 2 drones for social distancing announcement

https://www.whec.com/coronavirus/talking-drones-enforce-social-distancing-in-georgia/5699803/

Three drones deployed as Cauayan City, Philippines, contract its first COVID case

https://newsinfo.inquirer.net/1258287/drones-deployed-as-cauayan-citys-1st-case-alarms-residents

Tallinn, Estonia, deploy drones to combat spread of COVID-19

https://news.err.ee/1077276/tallinn-uses-drones-to-inform-people-about-coronavirus-restrictions

Wing Aviation completes more than 1,000 drone deliveries during COVID-19 pandemic

https://www.businessinsider.com/demand-for-wings-drone-deliveries-surging-due-to-covid-19-2020-4?IR=T

Manna Aero to trial drone delivery in Moneygall, Ireland, after Irish Aviation approval

https://www.forbes.com/sites/simonchandler/2020/04/03/coronavirus-delivers-worlds-first-drone-delivery-service/#7833cbf49579

CIRC collaborate on smart-platform-compatible drones for South Korea and Japan

https://www.thefastmode.com/technology-solutions/16866-kddi-lg-uplus-to-launch-smart-drone-in-japan-and-south-korea

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.

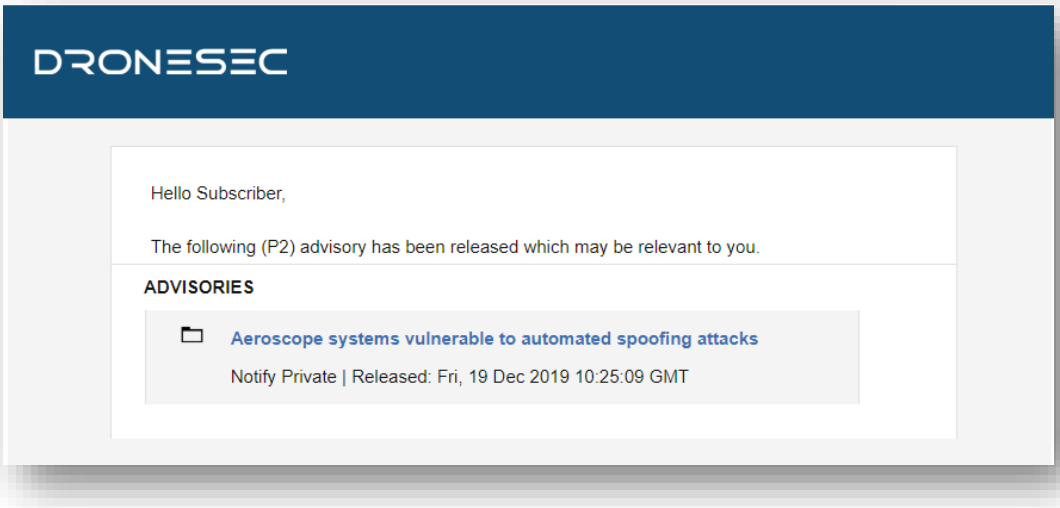


Figure 1 - A threat notification specific to a Notify customer's listed keywords.

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.