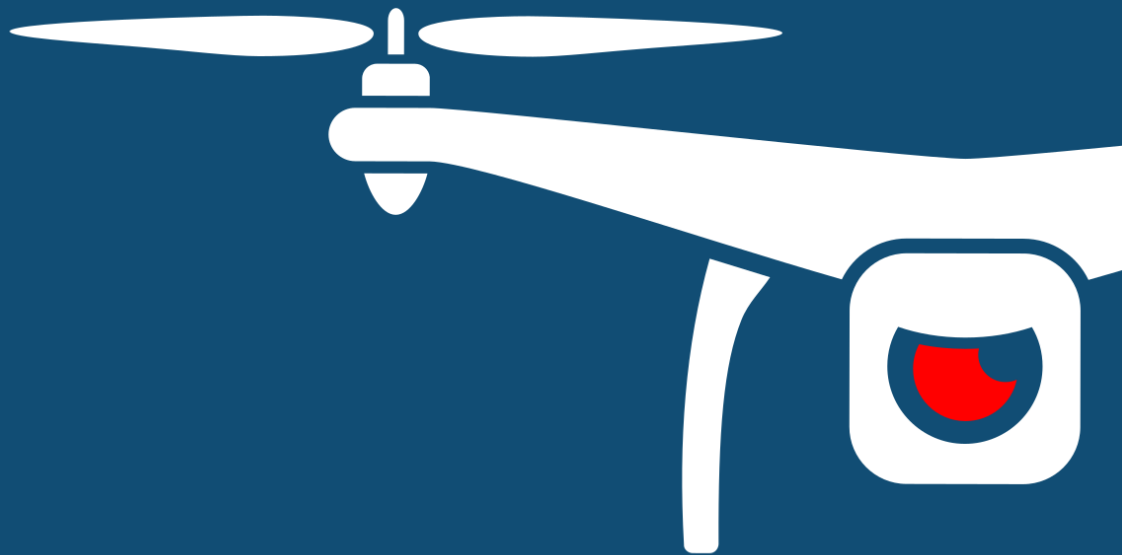




NOTIFY ISSUE #10

WEEKLY THREAT INTELLIGENCE

19 February 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

In Singapore, we had the opportunity to pitch DroneSec to a number of director heads at the Air Show. Within the pitch, I used coronavirus as an example and the extreme detail at which Singapore have used the method of 'contact tracing' to try and figure out where the person had been, who they had met, and what they had touched in an effort to locate potential infectious areas. This is a form of threat intelligence and focuses on digging into historical information to make informed guesses and assumptions about where threats might take place next time – a focus on prevention rather than simply response.

It's similar in a sense as to what we do at DroneSec. If we collect enough data, analyse the information and capture all the data points (location, model type, operator, time, pattern) we can start to look into the future and identify the possible threats that might take place, how they might look and how to best defeat them. This doesn't just serve customers without counter-drone controls but help refine those who do and continually compare and evaluate their process. Threat Intelligence is not optional when it comes to the security industry; this is as true for physical, cyber and warfare as it is for drones.

It was great being in Singapore and we had the opportunity to catch up with the likes of Oleg from DroneShield and Clay from Invisible Interdiction. The Counter-Drone industry is full of incredible experiences, personalities and technical minds and we were luckily enough to speak to students and hobbyists with simply a passion and interest in the area as well.

The Counter-Drone artefacts this week were mostly happening on the ground at the Singapore Air Show, and a few Q&A style interviews provide interesting reads and insights into some of the industry leader's current situations and roadmaps. We run our next 3-day DroneSec training course next month in March and we look forward to releasing a special Notify release for customers during that time.

- *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) ----- 6

1.4. Whitepapers, Publications & Regulations (P3)----- 7

1.5. Counter-Drone Systems (P4) ----- 7

1.6. UTM Systems (P5)----- 8

1.7. Drone Technology (P5) ----- 8

1.8. Informational (P5) ----- 9

APPENDIX A: Threat Notification Matrix----- 10

A.1. Objectives ----- 10

APPENDIX B: Sources & Limitations ----- 14

B.1. Intelligence sources ----- 14

B.2. Limitations----- 15



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)

Featured advisories were only accessible to Notify customers this week.

1.3. NEWS AND EVENTS (P3)

Syrian Army safely brought down five rebel drones via electronic warfare measures

Syria Military reported that five combatant drones operated by Takfiri militants were detected in the vicinity of several gas and energy facilities. The Syrian electronic warfare specialists were able to hack into the drones and land them safely before the payloads could cause any fire and material damage. No other specific details about the take-down methods have been made public yet.

<https://www.eurasiareview.com/17022020-syria-army-downs-five-drones-over-homs-oil-facility/>

Trials on using brain waves to operate drone swarms

The U.S. Defense Advanced Research Projects Agency (DARPA) is looking into using gamers' brain waves and eye movement to teach and operate hives of drone swarms. The aim is to utilise swarm intelligence for military applications to improve organisation and strategy among aerial and ground-based drones during missions in highly complex situations or environments.

<https://www.popularmechanics.com/technology/robots/a30855506/darpa-swarm-robots-video-game/>

FAA is investigating collision between a drone and helicopter at an off-road truck race

<https://www.verticalmag.com/news/camera-drone-helicopter-collide-during-off-road-race-in-california/>

Santa Cruz, USA County Sheriff's Office release first department drone use report

<https://www.ksbw.com/article/santa-cruz-county-sheriffs-office-releases-first-drone-use-report/30902276#>

Alice Springs, Australia police deploys drones to help tackle rising crime statistics

<https://www.katherinetimes.com.au/story/6630880/alice-springs-gets-drones-dogs-mounted-police-and-segways-katherine-got-loudspeakers/>

India police force to utilise drones for anti-terror operations in Jammu and Kashmir

<https://www.daijiworld.com/news/newsDisplay.aspx?newsID=674783>

Oregon law enforcement to utilise drones for firefighting and against crime

https://theworldlink.com/news/local/coos-bay-to-purchase-drones-for-police-and-fire/article_f2eb62b7-ff0e-5137-b520-2800655a86fc.html

Police in Tijuana Mexico utilise drones to fight crime and cartels in violent city

<https://www.uasnorway.no/fighting-crime-with-drones/>

Drone drops parcel containing phones, drugs into Trikala prison in Greece

<https://www.keeptalkinggreece.com/2020/02/02/drone-drugs-mobiles-trikala-prison/>

U.S. C5ISR awards project to create a "protected communications channel" for drones

<https://insideunmannedsystems.com/u-s-army-taps-persistent-systems-to-develop-secure-comms-for-robotic-and-autonomous-systems/>



1.4. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P3)

South Korea mandates registration of drones over 2 kilograms

South Koreans who own drones with a maximum take-off weight of over 2kg or weighing over 250 grams are required to register their drones starting 1 January 2021. The new law, to be promulgated in May 2020, was due to errant drone operators damaging property and cars without owing up to their mistakes. Some drone owners will also be required to take an online course, or a written and operation test and have 6-10 hours of flight experience based on the weight of their drones.

<https://www.zdnet.com/article/south-korea-to-strengthen-drone-registration-laws/>

Report: U.S. DoD and Pentagon Counter-Unmanned Aircraft Systems discussion

<https://news.usni.org/2020/02/14/report-on-pentagon-counter-drone-weapons>

Countering the Drone Threat: Implications of C-UAS Technology for Norway in EU/NATO Context

<https://www.prio.org/Publications/Publication/?x=12245>

IoT Security Institute launches framework for smart cities and critical infrastructure

<https://www.iotaustralia.org.au/2019/02/19/iotnewanz/iotsi-debuts-smart-cities-and-critical-infrastructure-security-framework/>

GRYPHON: Drone Forensics in Dataflash and Telemetry Logs

https://link.springer.com/chapter/10.1007/978-3-030-26834-3_22 (PDF available to Notify customers)

Optimal cruiser-drone traffic enforcement under energy limitation

<https://www.sciencedirect.com/science/article/abs/pii/S0004370218304909?via%3Dihub> (PDF available to Notify customers)

A Hierarchical Detection and Response System to Enhance Security Against Lethal Cyber-Attacks in UAV Networks

<https://ieeexplore.ieee.org/document/7890467> (PDF available to Notify customers)

1.5. COUNTER-DRONE SYSTEMS (P4)

Security intelligence and surveillance firm NSO purchases counter-drone organisation Convexum

<https://en.globes.co.il/en/article-nso-acquires-convexum-for-60m-1001318199>

Video: Rafael Counter-Drone system downing multiple DJI drones

<https://petapixel.com/2020/02/14/watch-an-anti-drone-laser-literally-fry-a-bunch-of-dji-drones-from-miles-away/>

TRD reveals Orion Counter-Drone tech to counter nano-swarms and non-ISM bands

<https://www.shephardmedia.com/news/digital-battlespace/singapore-airshow-2020-orion-first-join-bandwagon/>

DGS introduces new RF based drone detection and surveillance radar with 360 degrees field of view up to 15km range

<https://uasweekly.com/2020/02/16/dgs-announces-new-drone-detecting-surveillance-radar/>



DGS announces new drone detection surveillance radar

<https://www.unmannedairspace.info/counter-uas-systems-and-policies/dgs-announces-new-drone-detection-surveillance-radar/>

1.6. UTM SYSTEMS (P5)

Airbus joins others in Singapore UTM/UAM trails with Civil Aviation Authority support

<https://www.flightglobal.com/singapore-air-show-2020/airbus-and-the-civil-aviation-authority-of-singapore-explore-urban-air-mobility-solutions/136705.article>

FAA sets out next steps for UTM Pilot Program in Phase 1 summary report

<https://www.unmannedairspace.info/latest-news-and-information/faa-sets-out-next-steps-for-utm-pilot-program-in-phase-1-summary-report/>

Airbus UTM report highlights concerns around fair airspace access

<https://www.unmannedairspace.info/news-first/airbus-utm-report-highlights-concerns-around-fair-airspace-access/>

1.7. DRONE TECHNOLOGY (P5)

Detroit aims to create a highway for drones, six months test run in game plan

Detroit is planning to create a drone highway for the evolution of drone technology and logistics. Leaders from several aviation corporations and townships will be meeting to discuss on the game plan of test-running a drone highway between Metro Airport and Willow Run over a period of six months. The project aims to develop better policing and mapping of safe space for operations of drone and autonomous aircrafts.

<https://www.freep.com/story/money/2020/02/15/carol-cain-drone-highway-michigan/4765401002/>

Exyn Technologies introduces drones which can fly autonomously in GPS-denied environment

Exyn Technologies has built a code which allows drones to detect and gather critical information of their surrounding in real-time for situation awareness. Information collection includes high-fidelity 3D maps, human and object detection, allowing the drones to navigate around autonomously in a GPS-denied environment.

<https://www.c4isrnet.com/unmanned/2020/02/14/can-scout-drones-be-programmed-with-new-tricks/>

Flirtey boosts drone delivery services with patented parachute deployment system to reduce risk of safety implications

<https://uasweekly.com/2020/02/16/flirtey-granted-patent-enhances-safety-in-drone-delivery/>

<https://patents.google.com/patent/US10112721B2/en?q=flirtey&assignee=Flirtey+Holdings%2c+Inc.&status=GRANT>

Parrot and RIIS collaborate to develop AI and thermal technology

<https://mitechnews.com/drones/riis-parrot-partner-to-develop-drone-ai-technology/>



1.8. INFORMATIONAL (P5)

Police in Shenzhen, China use UAV's with QR codes to reduce human contact with coronavirus

(Images available to Notify customers)

Drone helps find blind man lost in woods within 30 minutes of searching

<https://www.ctpost.com/local/article/Enfield-police-lost-blind-man-found-with-drones-15060714.php?src=posthpcp>

DJI speaks on beneficial impacts of drones, data security and remote ID

<https://dronedj.com/2020/02/14/djis-brendan-schulman-talks-about-coronavirus-remote-id-data-security/>

DJI pledges 1.5 million to spray disinfectant around China to fight against Coronavirus

<https://www.itp.net/business/91440-dji-is-using-drones-to-help-fight-the-coronavirus>

Drone pilot helps community search for missing 11-year-old

<https://denver.cbslocal.com/2020/02/14/gannon-stauch-missing-boy-drone-pilot/>

Downed Chinese drone found in Cambodia linked to secret visit to naval base by Chinese military official

<https://www.abc.net.au/news/2020-02-05/secret-chinese-delegation-visited-cambodian-naval-base/11928184>

Thermal and spotter drones used by Miami County SWAT teams

<https://www.daytondailynews.com/news/local/miami-county-sheriff-office-use-drones/8v6sOqHr8Jie4qqIMHESdO/>

U.S. Navy seize Iranian-made munitions, unmanned aircraft components in boat

https://www.navy.mil/submit/display.asp?story_id=112097

Threats and legislation barriers prevent drone innovation in NZ

<https://www.newsroom.co.nz/2020/02/11/1028575/drones-in-nz-have-their-own-traffic-delays>

Q&A: Drone security and counter-drones with Brett Velicovich

<https://mydeardrone.com/interviews/brett-velicovich-on-counter-drone/>

Q&A: Drone threats and counter-drone technologies with Robert Fink

<https://tulodz.pl/extra,inteligentne-technologie-i-czlowiek,kiedy-zagroza-nam-drony-inteligentne-technologie-i-czlowiek-wideo,new,mg,73,79.html,4683>

Counter-drone market to grow in size by about \$4.3 billion by 2026

<https://newsus.app/anti-drone-market-size-is-about-us-443-billion-by-2026/>



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.

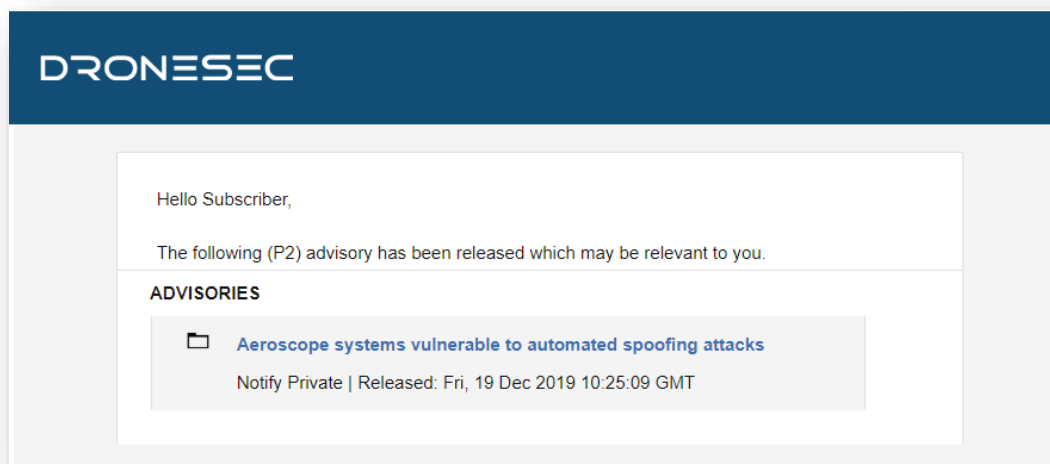


Figure 1 - A threat notification specific to a Notify customer's listed keywords.

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: <ul style="list-style-type: none">• Be known as UAS¹, UAV², RPAS³...• Weigh 50g all the way to 250kgs• Are automated or manually piloted• Have associated devices, software or infrastructure |
| CUAS | Counter-UAS systems that might: <ul style="list-style-type: none">• Be known as Counter-Drone or C-UAV |

¹ UAS: Unmanned Aerial System

² UAV: Unmanned Aerial Vehicle

³ RPAS: Remotely Piloted Aerial System



| | |
|-----|---|
| | <ul style="list-style-type: none"> • Detect and/or respond to drones • Be standalone, hand-held, static or integrated with a UTM⁴ or PSIM⁵ system • Have associated systems, software, infrastructure and communication protocols |
| UTM | Universal Traffic Management system that might: <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> - 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 dronsec.xyz, dronsec.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@dronsec.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.

