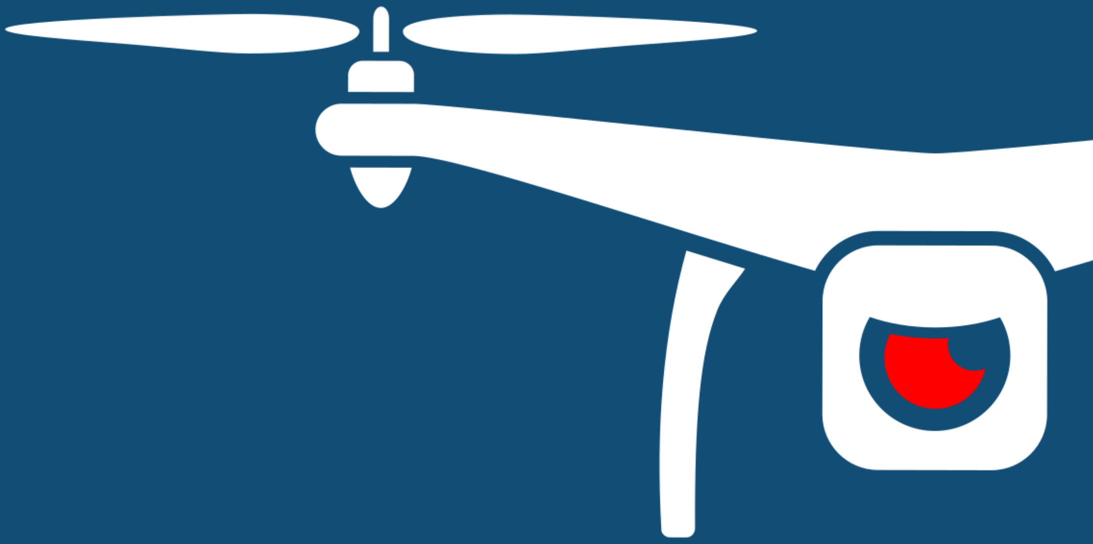
DRONE SEC

NOTIFY ISSUE #100 (PUBLIC)
WEEKLY THREAT INTELLIGENCE

11 Nov 2021 | v1.0 RELEASE



UAS HACKING, HARDENING AND DEFENCE

DOCUMENT CONTROL

PREPARATION

DroneSec (dronesec.com)

Threat Intelligence Team

Email: info@dronesec.com

TABLE OF CONTENTS

1. Threat Intelligence ---- 4
1.1. Featured Advisories ---- 4
1.2. Non-Conflict News and Events (P3) ---- 12
1.3. Conflict News and Events (P3) ---- 14
1.4. Socials (P3) ---- 15
1.5. Whitepapers, Publications & Regulations (P4) ---- 17
1.6. Counter-Drone Systems (P4) ---- 17
1.7. UTM Systems (P5) ---- 18
1.8. Informational (P5) ---- 18

1. THREAT INTELLIGENCE

1.1. FEATURED ADVISORIES

The prioritisation table and how we filter, analyse and visualise the intelligence we collect is located at the end of the document.

Intrusion and Trespass	Priority
Modified anti-forensics DJI Mavic 2 with copper wire discovered near electrical grid (UPDATE)	**P2**

Summary

This is an updated artefact, observed by DroneSec in August 2020.

A Joint Intelligence Bulletin by the United States government revealed that a recovered crashed drone was used with the potential intention of deliberately disrupting an electrical substation in July 2020.

Overview

In a combined joint intelligence report by the United States Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS) and the National Counterterrorism Center (NCTC), a DJI Mavic 2 drone was recovered on the roof of an electrical substation in Pennsylvania. The drone was modified to have two pieces of nylon rope attached to the arms of the drone and a copper wire on the other end of the ropes. It was also noted that the drone had its camera, internal memory card and any identifying markings removed. The report goes on to mention that the drone was likely being used to specifically target and disrupt the substation as the copper wire could short circuit the transformers or distribution lines. The drone was also appeared heavily worn, indicating multiple uses before it was modified for this single flight into the substation. The drone operator for this incident was not caught.

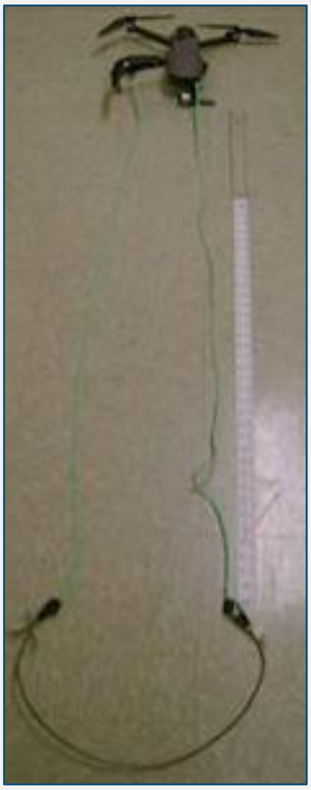


Figure 1: Incident DJI Mavic 2 used to disrupt substation

Analysis

Deliberate efforts were taken to purposely remove the drone's camera, internal memory card and identifying markings by the drone operator. This indicates the intention to conceal their identity and make it difficult for law enforcement agencies to trace the drone's origins. Many components, such as the camera or batteries, can be analysed to determine the source or origin and lead to attribution of the operator.

The electrical substation is located in between two places of interest with a high number of public visitor activity. Sometimes, operators choose to take off at areas away from busy public locations to avoid detection and reporting by the public.

The operator may have had had to rely on a visual line of sight as the camera was removed, removing the controller-based visual video of the drone's position. However, as it is difficult to gauge distances and height from a standoff location, the operator, thinking the drone was directly above, may have lowered it onto the roof of the building instead. Alternatively, the operator could have created an autonomous, pre-defined flight path which the drone was able to follow without pilot visuals and input; however, this is inconsistent with the eventual location in which the drone was observed.

This may suggest that the operator could not have been standing at a location perpendicular to the substation and the adjacent building as that would have given them full awareness of which building the drone was above. This could infer the operator was standing at a location parallel to both buildings, which caused the inaccurate descension onto the adjacent building instead of the substation.

There are residential houses located on both sides where the view is parallel to the substation and its adjacent building. As the substation is covered by surrounding trees, it may have been possible for the drone operator to operate the drone from an upper storey residential apartment or roof in order to have clear line of sight of the drone above the tree line.

There are also additional open areas in the surrounding location with public access that may have allowed the operator to pilot from.

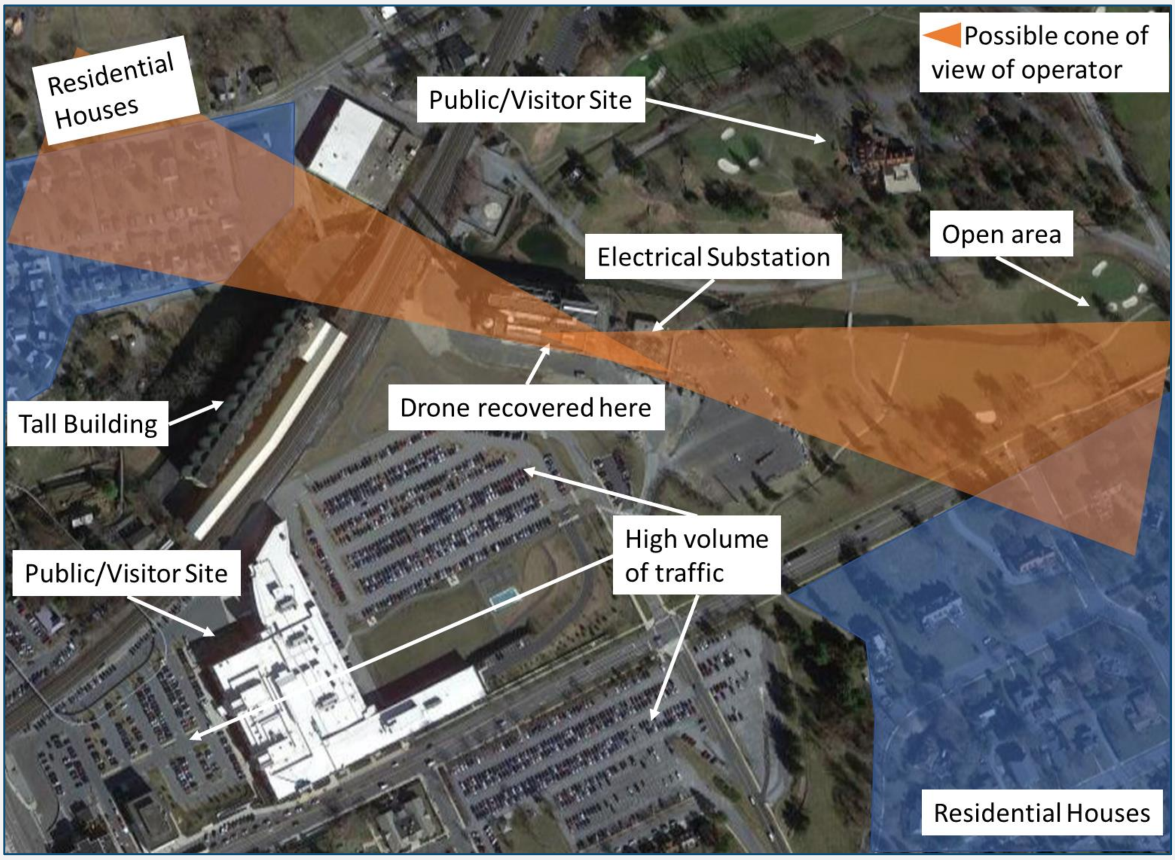


Figure 2: Possible locations (blue and orange areas that intersect) where the drone operator might have been

Recommendations

Defending critical infrastructure from drones located in close proximity to public areas requires careful consideration and layered defences. Where a Counter-Drone system may not be possible, DroneSec recommends critical infrastructures to have an Incident Response plan to ensure quick business continuity when drone incursions occur. Where counter drone systems can be effectively implemented, having a standard operating procedure for collecting digital and physical evidence is an important inclusion, with war games or table-top exercises being conducted during the implantation phase.

Depending on their environment and threat profile, Critical Infrastructure facilities should treat drones with an equal or greater priority around budgeting as current Hostile Vehicle Mitigation procedures. Drones can be purchased for as low as $200 and bypass many physical and ground-based perimeter defences, requiring drone detection and mitigation technologies. Existing protocols for HVM may not apply to aerial-based surveillance or direct attacks as seen in this scenario, with a low-entry barrier to financing or skills required in order to conduct such an attack.

Reference

https://amp.cnn.com/cnn/2021/11/04/politics/drone-pennsylvania-electric-substation/index.html

https://www.thedrive.com/the-war-zone/43015/likely-drone-attack-on-u-s-power-grid-revealed-in-new-intelligence-report

Intrusion and Trespass	Priority
Three explosive-laden drones by Iranian-backed militia strike Iraqi Prime Minister’s residence	**P2**

Summary

Explosive laden drones targeted the Iraqi Prime Minister's residence in Baghdad, destroying properties and injuring bodyguards.

Overview

Three armed drones were reported targeting the Iraqi Prime Minister's residence in Baghdad; however, two of the drones were shot down by Iraqi defences and one managed to successfully hit the compound. The drones were said to have been launched near the Republic Bridge on the River Tigris, which is just about 2km away from the Prime Minister's residence. The strike caused damage to a vehicle and the residential compound with six security guards injured and no casualties. The strike was assumed to be from Iranian backed militia groups; however, no group has stepped forward to claim responsibility yet. The social media on twitter was quick to point out that the payload found from this incident (second photo below) was observed previously in another strike in July 2020 and July 2021 strike within the Green Zone by the Shiite militias (third photo below). However, this information was not confirmed by official sources.

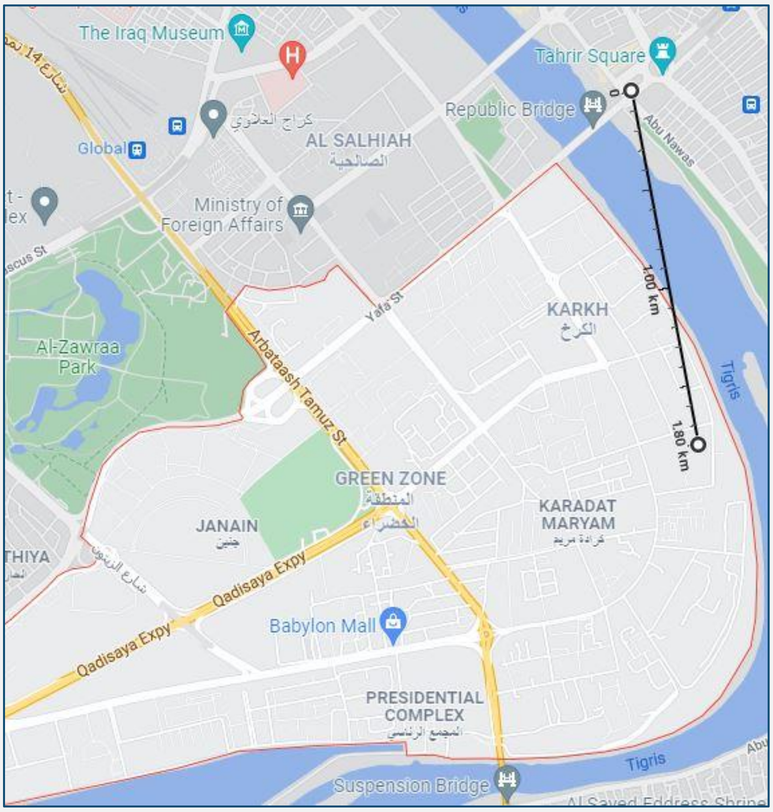


Figure 3: Distance of the bridge to the Prime Minister's residence

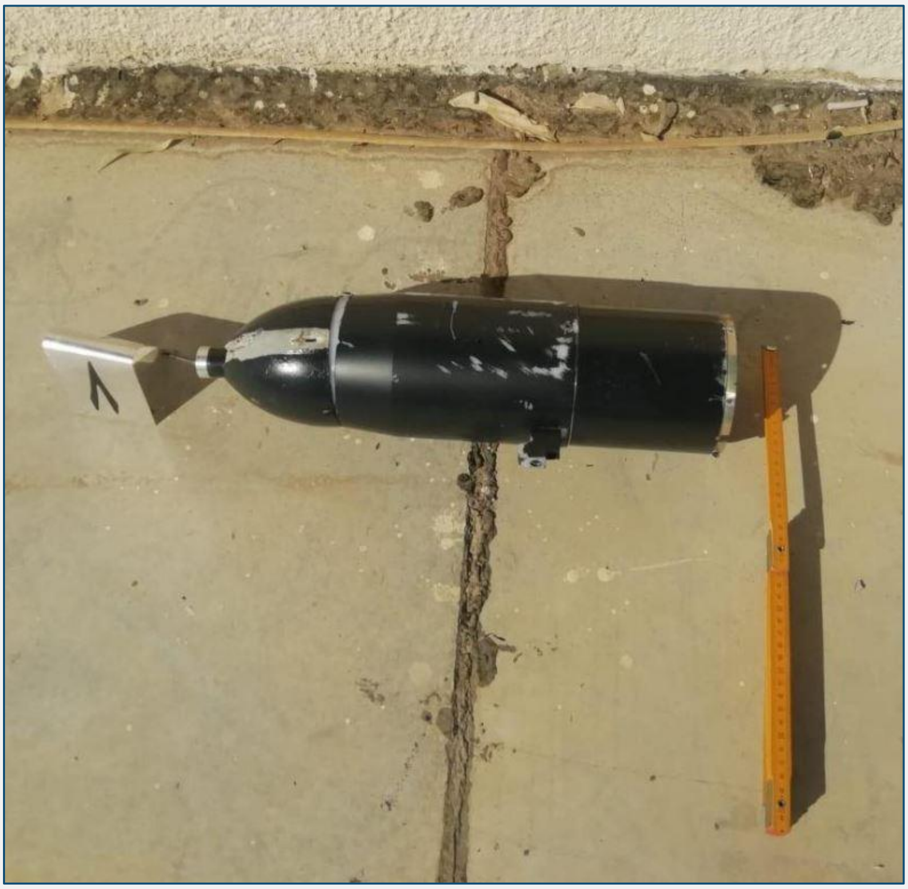


Figure 4: Bomb shell casing recovered nearby after the blast

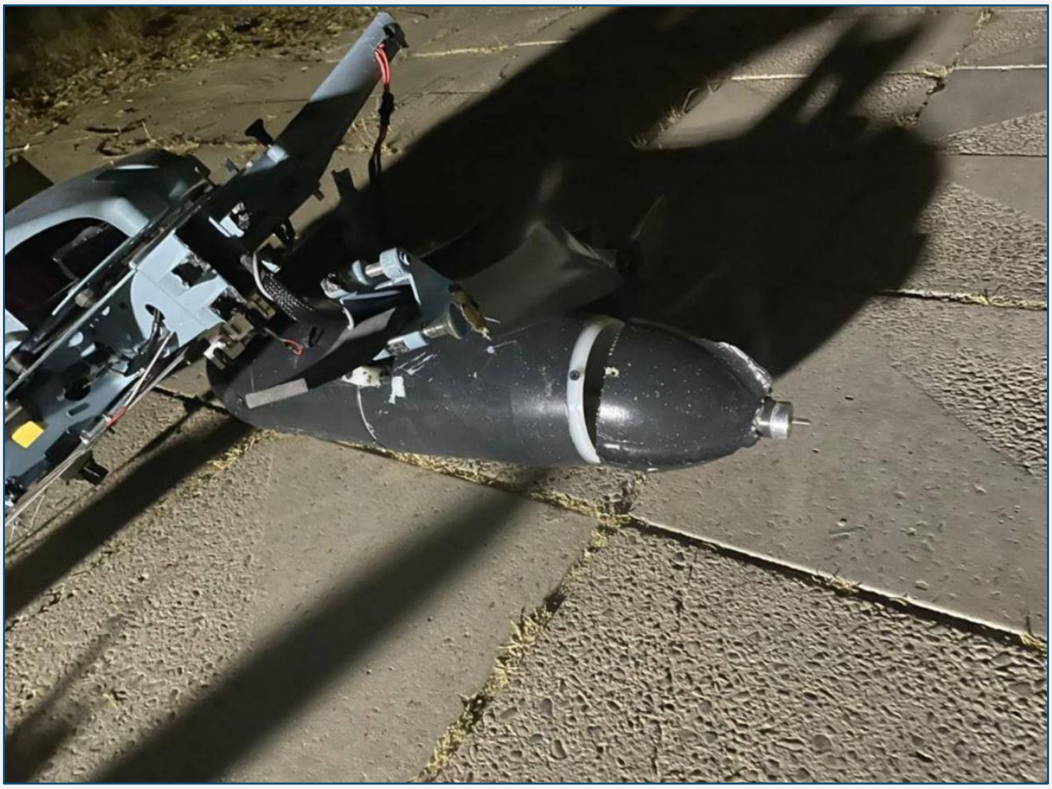


Figure 5: JULY 2021: Image of the similar bomb (and drone) used in a previous attack

Analysis

The Green Zone is one of the most heavily protected areas in Iraq with counter drone systems in place and drone jamming hardware available for use. These systems are deployed on a large scale, including portable counter drone jammer guns, vehicle mounted units and fixed installations. It was pointed out that the drones were not susceptible to jamming, indicating that these drones may have been on a pre-programmed flight path with no direct link between drone and operator, causing jammer guns to be ineffective. This is not the first time heavy-lift, GPS pre-programmed drones with armed payloads have been used within Iraq (Jadriyah, July 2020 - https://twitter.com/AuroraIntel/status/1286339193829044224/photo/1).

However, even pre-programmed flights are susceptible to GPS jamming. Some drones are not susceptible to GPS/GLONASS jamming yet rely on visual and other sensors to position themselves in relation to the environment around them; however, these types of 'dark' drones may rely on tactile user input on frequencies or channels not countered by the jammers.

The explosive was stated to have a sophisticated fusing system and is armed by a vane which spins as the bomb falls. The detonator in the rear of the bomb becomes live when the vane spins and is set off by impact. Reports have also stated that the custom-made warhead appears to be armour piercing shaped charge which could possibly be intended to strike through a roof rather than hitting individuals in the open. However, the bomb struck a vehicle in a garage instead of a building.

Open-source discussion has also reported officials chatter reporting that whilst a C-RAM was in-place, the drones were outside the reach of its detection range and was not automatically activated. This may indicate that the drones were flown at a low enough in altitude to the ground that it was not possible for the C-RAM to engage.

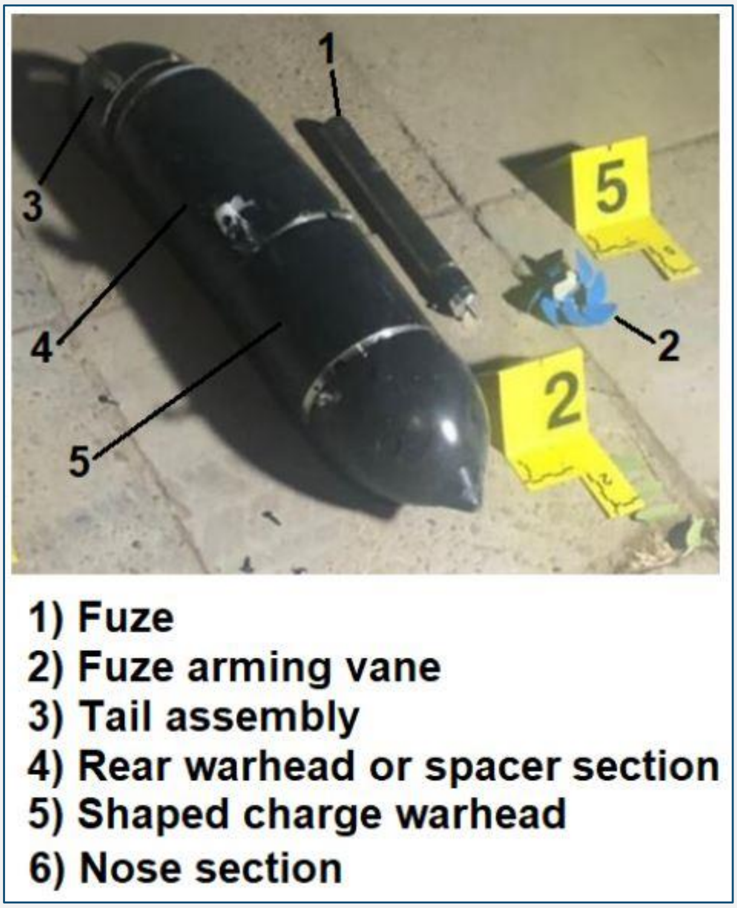


Figure 6: Breakdown of the components of the bomb - https://twitter.com/blueboy1969/status/1457479574758076417

Autonomous drones have no communicative link between the operator and the drone which means that the operator will not be able to alter his route once the drone has taken off. However, that also means that the drone may bypass being intercepted by third parties until it completes its mission. If the mission did in fact utilise 'dark' drones or those unsusceptible to the current jamming technology, it demonstrates a maturity in understanding and operational capability of those coordinating the attack. Terrorists and militia groups are continually able to understand, apply and counter the benefits and cons of drones and counter drone systems within the field, and mitigation systems need to be able to utilise soft-kill methods for targeting targets that are below their vertical range of targeting.

Recommendations

DroneSec recommends law enforcement and military agencies to adopt multi-layered counter drone systems, and to always have layered defences when protecting assets or critical infrastructures against drone intrusions. A layered defence will help to better counter against customised and modified drones to varying degree, taking them down with both hard kill and soft kill methods. A combination of detection sensors (radar, RF and visual) as well as mitigation types (exploitation, RF/GPS jamming and spoofing, kinetic) with an active threat intelligence program can prepare for unique and advanced use cases.

Reference

https://www.forbes.com/sites/davidhambling/2021/11/08/heres-what-we-know-about-the-drone-attack-on-iraqs-prime-minister/amp/

https://twitter.com/blueboy1969/status/1457479574758076417 (open-source munition analysis)

Intrusion and Trespass	Priority
Yuma Border Patrol seize Mexican drone with 3kg of narcotics and GPS tracker at Arizona border	**P2**

Summary

Border Patrol agents in Yuma Sector seized a drone with 6.5 pounds (3kg) of narcotics and a GPS tracker over the Arizona-Mexico border.

Overview

Yuma Sector Border Patrol agents seized a drone, possibly a DJI Matrice 600 Pro, carrying 3kg of narcotics attempting to cross the border into Yuma, Arizona. Law enforcement officers discovered that the payload of the drone, sealed in black plastic bag, also had a GPS tracker inside of it. It was reported that such packages of narcotics are often equipped with trackers to allow smugglers waiting on the other side of the border to easily locate the packages after they are dropped. The drone and the contraband were seized, but the operator was not found.

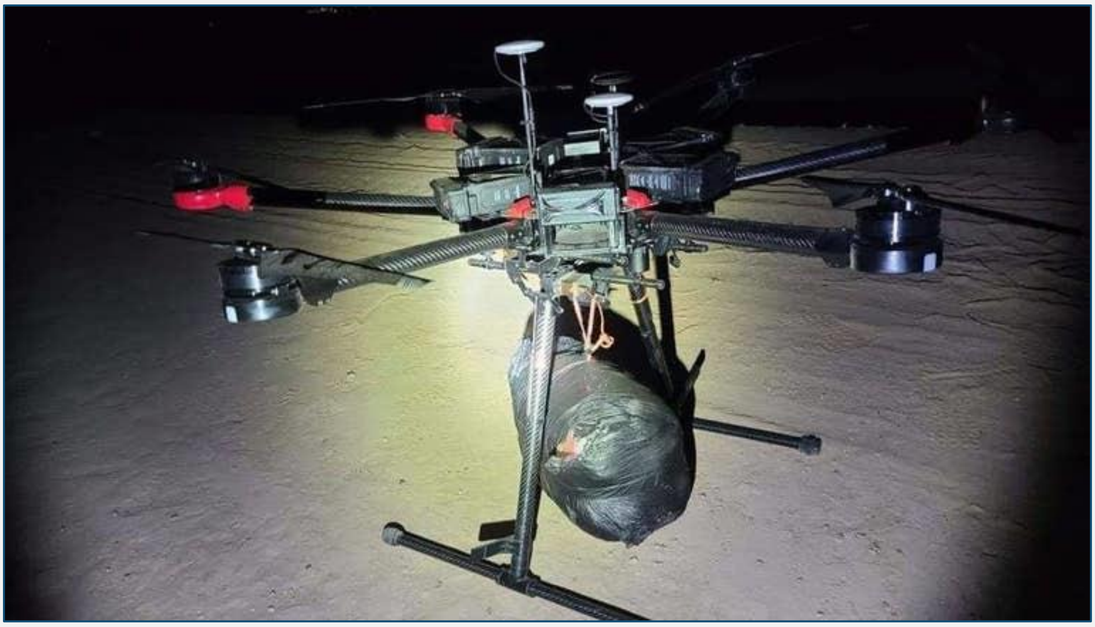


Figure 7: The heavy-lift drone seized, likely a DJI Matrice 600 Pro with payload dropping mechanism

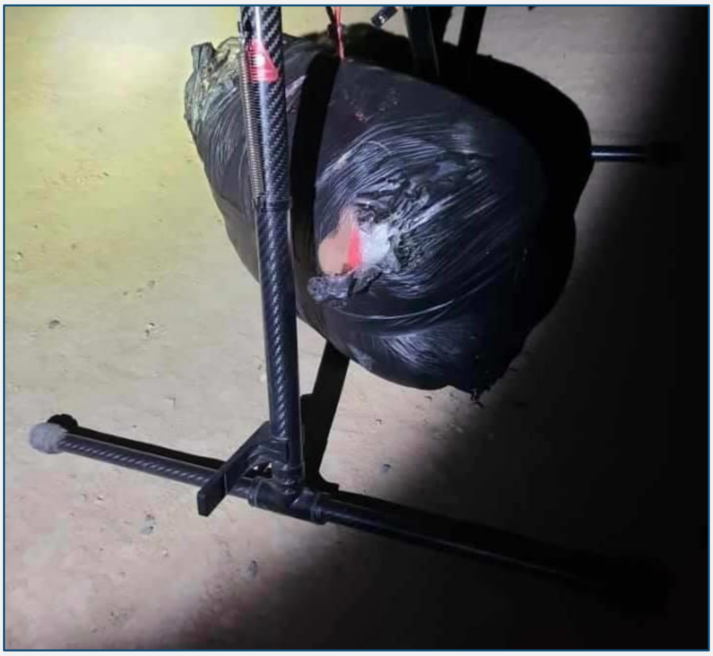


Figure 8: Contraband in a black plastic bag attached to the undercarriage of the drone

Analysis

It is important to note that the DJI Matrice is a drone that is usually used by commercial organisations for heavy duty drone operations. This drone costs around USD$4,500. For the criminal in this incident to possess one, the drone could have belonged to a commercial organisation, was stolen, or purchased with cartel funding. Increasingly, crime gangs and cartel groups outside of conflict areas are utilising more expensive drones, indicating a larger organisation focus with the financial backing to procure such systems.

The Mexico-United States border have seen multiple drone incursion over the past years. It is becoming more common for borders globally to experience contraband delivery via drones, which could indicate a rise in threat actors adopting the use commercial-off-the-shelf (COTS) drones as part of their modus operandi in committing crimes. There is little risk of being apprehended as drones and operators are separated by distance and wireless transmissions, coupled with a low skill barrier to conduct a successful drone operation.

Threat Actor Group

USA-Mexico Border Smuggling Groups: https://help.dronesec.com/en/articles/4637822-usa-mexico-border-smuggling-groups

Recommendations

Yuma Sector Border Patrol have a drone security management plan and counter drone systems are in place to detect and deter against such illegal drone operations. However, tackling drone-related border incursions continue to be an uphill battle as offenders can always vary their ingress and egress routes to avoid detection. Due to the low price-point of drones, it is possible these drones were used as a one-way mission. In this case, forensic analysis of the drone's telemetry may be useful, potentially aiding in the discovery of the launch location of the drone, and positioning counter-drone systems in that flight corridor. Event analysis from the drone data and video footages from current and past drones captured could lead to the recognition of patterns and trends (such as origin of flight, time of day etc) which may help provide the modus operandi of rogue groups and may aid in the arrest of the operator.

Reference

https://www.fox10phoenix.com/news/yuma-border-agents-seize-drone-carrying-heroin-gps-tracker

https://www.facebook.com/USBPYumaSector/posts/190003853317229

1.2. NON-CONFLICT NEWS AND EVENTS (P3)

Six Turkish drones for agricultural purposes seized in Somalia after laws ban use of drones

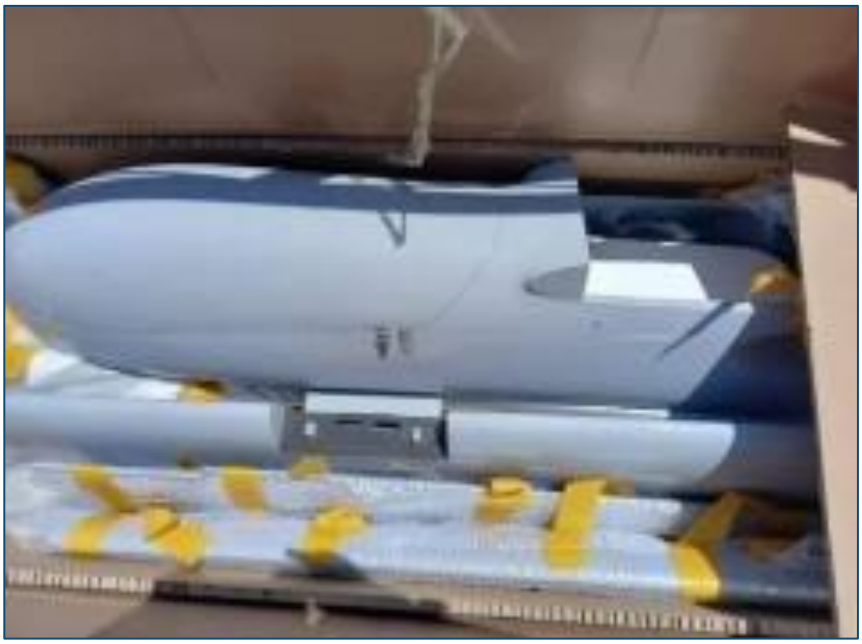


Figure 9: Turkish drone seized by Somalian authorities

https://allafrica.com/stories/202111040668.html

https://t.me/auraxchan/31720

India border forces finds 11kg of narcotics in an agricultural field, possibly Pakistani drone drop

https://www.republicworld.com/india-news/general-news/punjab-bsf-recovers-heroin-worth-rs55-crore-near-indo-pak-border-in-fazilka-district.html

Bangladeshi arrested for flying drone illegally in sacred temple for YouTube video, Sri Lanka

http://www.colombopage.com/archive_21B/Nov05_1636134103CH.php

Report highlights contraband drone deliveries occur weekly at Wandsworth Prison, England

https://www.standard.co.uk/news/london/drones-drug-deliveries-wandsworth-prison-watchdog-b964669.html

Drones intrude into Mars Desert Research Station at Utah, disrupting training and research

https://screenrant.com/mars-simulation-utah-tourism/

CASA reports increased drone activity around Gold Coast Airport at beachside locations

https://www.casa.gov.au/media-release/unsafe-drone-activity-gold-coast-region-aviation-regulators-radar

Man fined for flying unauthorised and unregistered drone for roof inspection, Singapore

https://www.straitstimes.com/singapore/courts-crime/ntu-housing-manager-fined-7500-for-flying-drone-to-check-if-hall-rooftop-was

Possible drone flights over neighbourhood observed almost every day, Dietzenbach, Germany

https://www-op--online-de.translate.goog/region/dietzenbach/spionage-unter-nachbarn-91098395.html?_x_tr_sl=de&_x_tr_tl=en&_x_tr_hl=de&_x_tr_pto=nui

Prison officers takes down contraband filled DJI Matrice 300 with jammer guns, Brazil

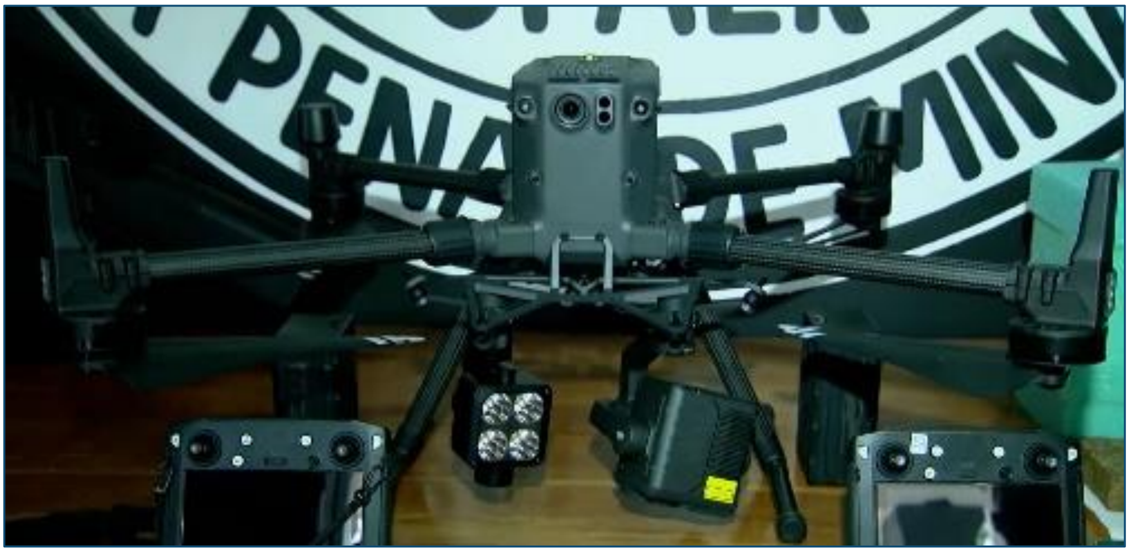


Figure 10: DJI Matrice 300 used to transport contraband

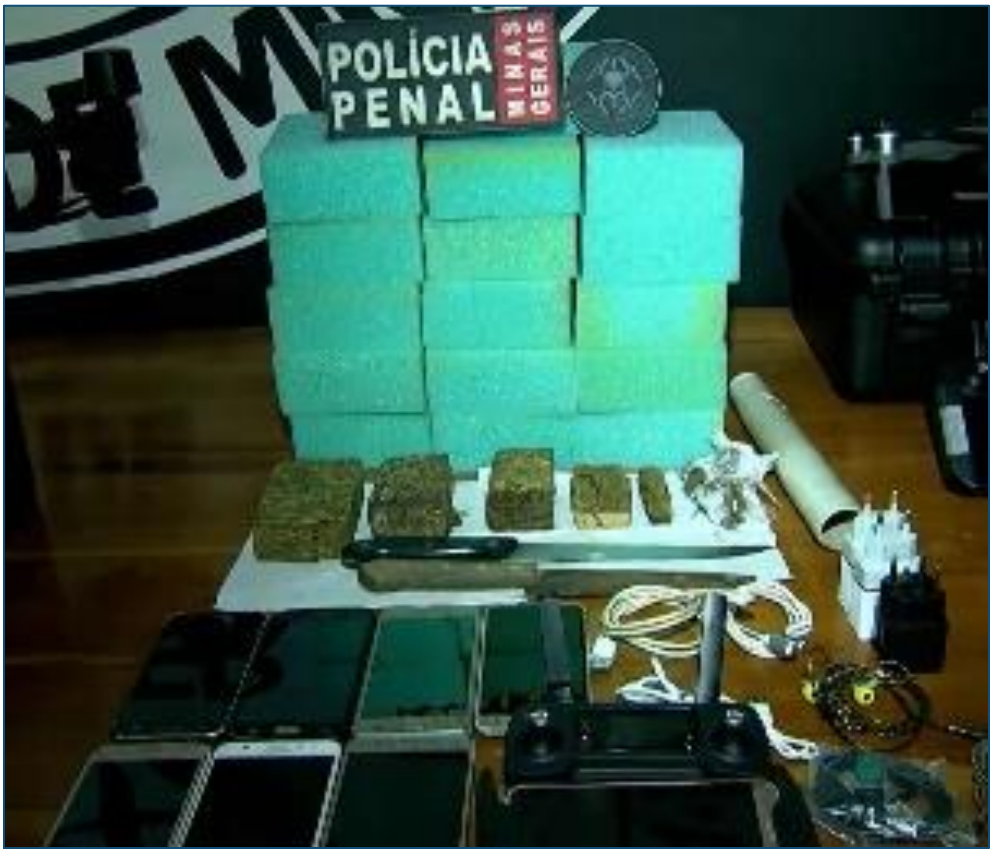


Figure 11: Contraband seized by Brazilian prison officers

https://noticias.r7.com/minas-gerais/balanco-geral-mg/videos/drone-e-derrubado-por-policiais-penais-apos-sobrevoar-penitenciaria-04112021

Unlicensed self-assembled fixed-wing drone crashes into residential unit, China

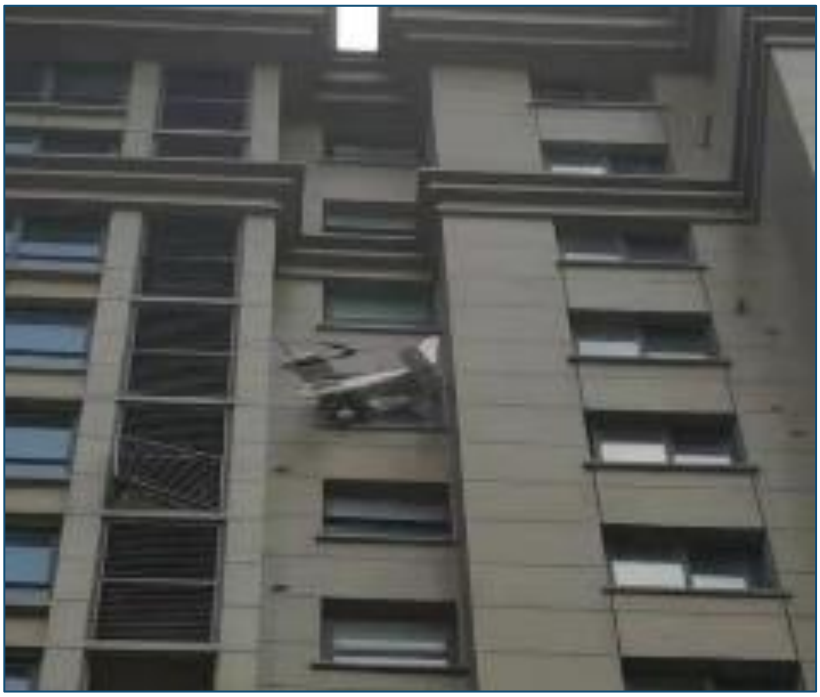


Figure 12: Custom built drone that crashed into a residential unit in China

https://kanzhaji.com/news/flysafe/62969.html

Chinese drone programmer arrested for testing custom made drone in No-Fly-Zone, Shanghai

https://kanzhaji.com/news/flysafe/62957.html

1.3. CONFLICT NEWS AND EVENTS (P3)

Saudi Air Defences destroy Houthi drone targeting Jazan

https://www.arabnews.com/node/1962016/saudi-arabia

Arab Coalition destroys Houthi suicide drone targeting Khamis Mushait, Saudi Arabia

https://saudigazette.com.sa/article/613233

Another Houthi drone targeting Abha Airport was destroyed by Saudi Air Defences

https://english.alarabiya.net/News/gulf/2021/11/06/Saudi-air-defenses-intercept-Houthi-drone-headed-for-Saudi-s-Abha-airport

Israel Iron Dome shoots down Hamas drone flying out at sea from Gaza Strip

https://www.timesofisrael.com/iron-dome-shoots-down-hamas-drone-flown-out-to-sea/

Yemen reports shooting down US military drone over Marib

https://en.abna24.com/news//yemeni-army-shoots-down-us-spy-drone-over-marib_1196945.html

1.4. SOCIALS (P3)

Initial report claims Iranian Armed Forces shot down US drone near coast of Oman

https://t.me/Aq701/8261

Reports of Iranian Armed Forces warning US drones during Iran military exercise

https://thehill.com/policy/defense/580673-iran-says-its-military-warned-off-us-drones

Houthi Rased-like drone shot down in west of Taiz Governorate, Yemen

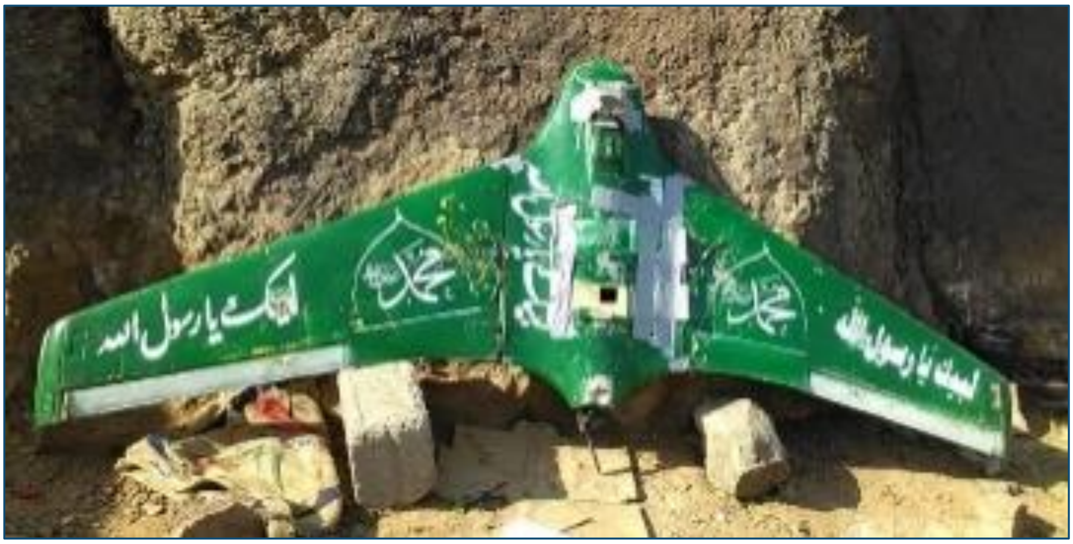


Figure 13: Rased drone shot down by Yemeni Army

https://twitter.com/South24_net/status/1456255282502266880

Lightweight anti-drone jammer gun, LPD-801 by PPSh Laboratory showcased in Russia

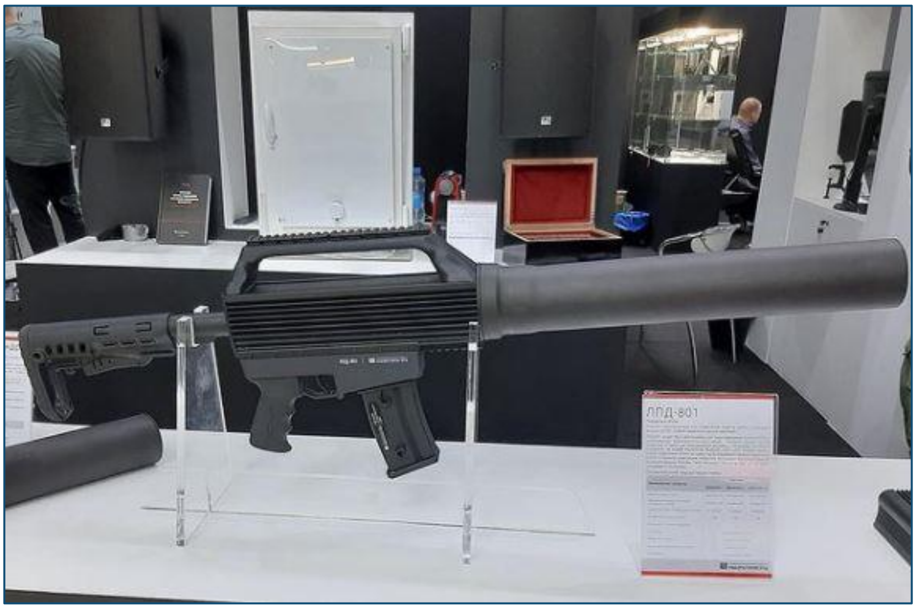


Figure 14: Lightweight anti-drone gun, LPO-801

https://www.instagram.com/p/CVdF2msLlXk/

DPR soldier injured with numerous shrapnel wounds, possible from payload dropped by drone

https://t.me/donbassinsider/2575

Iranian Army releases video of suicide drone, Arash, successfully destroying simulated target

https://t.me/rtnoticias/22382

DIY drone tutorial made with commercial off the shelf radio receivers, motors and circuit board

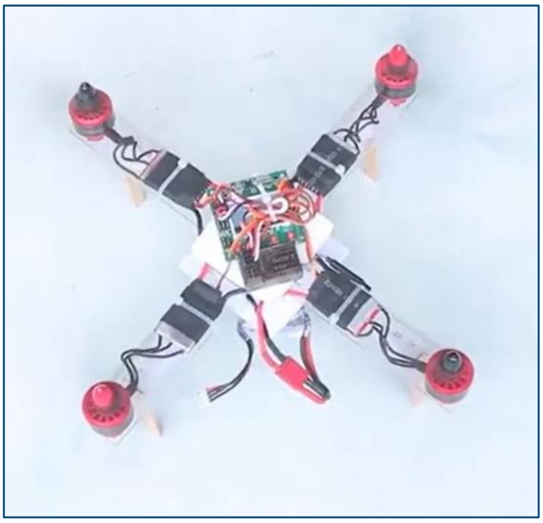


Figure 15: DIY drone tutorial with easily available materials and components such as rubble

https://www.facebook.com/107873611105828/videos/1008769373299213c

Primitive drone shot down by Assad militia over Al-Ghab Plain, Syria

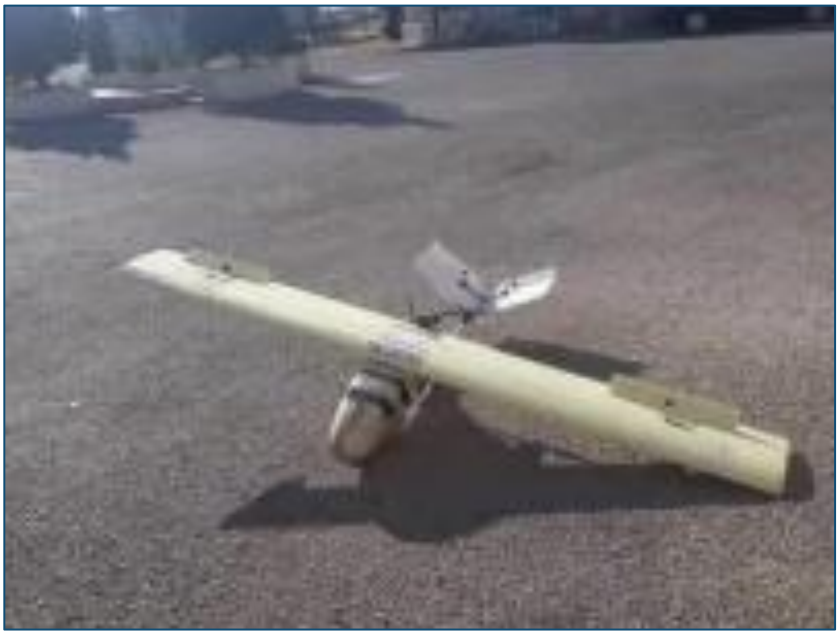


Figure 16: Drone seized by Syrian Army

https://twitter.com/tommycats4/status/1457997005792464896

Live-fire sniper and counter-drone training conducted at Sleep Train Arena, Sacramento USA

https://www.linkedin.com/posts/andy-morabe-2552451_training-dronekiller-tacflow-activity-6859445249648029696-YX4W

Commercial drone flight narrowly misses power lines, flies over public, UK (livestream)

https://www.facebook.com/watch/live/?ref=watch_permalink&v=205476278362098

Drone flies over Leanne Field stadium NFL game, Edon, Ohio, USA (livestream)

https://www.facebook.com/coty.arkwright/videos/3086956888296523/

1.5. WHITEPAPERS, PUBLICATIONS & REGULATIONS (P4)

Autonomous Drones Have Attacked Humans. This Is a Turning Point (Commentary)

https://www.popularmechanics.com/military/weapons/a36559508/drones-autonomously-attacked-humans-libya-united-nations-report/

Operative describes how Mexico's cartels use drones to attack enemies and smuggle drugs (Commentary)

https://www.businessinsider.com/how-mexicos-cartels-are-using-drugs-for-attacks-drug-smuggling-2021-5

Increase in illegal drone flights causes grounded flights, issues for firefighters (Commentary)

https://www.kcra.com/article/dangerous-drones-increase-in-illegal-drone-flights-causes-grounded-flights-issues-for-firefighters/38139410

Armed drones in future wars: ADF needs asymmetric technology (Commentary)

https://www.theaustralian.com.au/special-reports/armed-drones-in-future-wars-adf-needs-asymmetric-technology/news-story/ebdff4f829217b4a7a65751e720851a7

Could the Next 9/11 Be Caused by Drones? (Commentary)

https://www.newsweek.com/could-next-9-11-caused-drones-1647249

1.6. COUNTER-DRONE SYSTEMS (P4)

FAA begins drone tests to protect airports at the Atlantic City International Airport, New Jersey

https://www.kcra.com/article/faa-begins-first-ever-drone-tests-to-protect-airports/38166246

BlueHalo acquires Citadel Defense counter drone company

https://bluehalo.com/press_release/bluehalo-solidifies-leading-position-in-counter-uas-with-acquisition-of-citadel-defense/

Black Sage introduces 35km range jammer system, Goshawk, to counter against drone threats

https://blacksagetech.com/repository/black-sages-goshawk-delivers-ew-jamming-for-the-united-states-air-force-at-ranges-exceeding-35km

How sensor networks and mobile mesh networking are countering the UAS threat (commentary)

https://thelastmile.gotennapro.com/how-sensor-networks-and-mobile-mesh-networking-are-countering-the-uas-threat-2/

1.7. UTM SYSTEMS (P5)

French aviation school (ENAC) acquires UTM platform to include drones into training simulation

https://www.unmannedairspace.info/latest-news-and-information/enac-the-french-training-school-adds-utm-platform-to-train-future-air-traffic-controllers/

Skyroads, Altitude Angel and OneSky joins Hyundai consortium to develop ConOps for AAM

https://www.unmannedairspace.info/latest-news-and-information/altitude-angel-joins-urban-air-mobility-division-of-hyundai-motor-group-consortium-to-co-develop-aam/

1.8. INFORMATIONAL (P5)

Russia's first drone test site to open next year near Orlovka airfield

https://www.thedefensepost.com/2021/11/03/russia-drone-test-site-postponed/

Aerial surveillance video from FBI drone used as evidence to convict homicide trial

https://edition.cnn.com/2021/11/03/us/kyle-rittenhouse-trial/index.html

Nottinghamshire PD finds missing woman unconscious with help of drone

https://westbridgfordwire.com/video-shows-police-drone-locate-vulnerable-missing-woman-unconscious-in-a-field/

French National Police RAID unit equips drone swarm technology to map CBRN threats

https://www.forcesoperations.com/le-raid-se-dote-dessaims-de-drones-renifleurs/

For Appendix items please click this link.