Criminal Justice Testing and Evaluation Consortium
A Program of the National Institute of Justice

NIJ National Institute of Justice
STRENGTHEN SCIENCE. ADVANCE JUSTICE.

Contraband and Drones in Correctional Facilities

An overview of technologies and issues associated with detection and response

This technology brief is part of a series that focuses on contraband in correctional facilities. The series offers insight into the types of contraband and associated technologies and products used to remotely detect contraband on people, in vehicles, in mail, and in the corrections environment. This brief provides an overview of the options and challenges associated with detecting and mitigating drone-delivered contraband in correctional facilities in the United States (see **Figure 1**).

Key Takeaways

- The threat of contraband associated with drones is escalating with the evolution of the technology, which enables drone operators to carry larger payloads, fly faster and for longer distances, and operate at lower levels of investment. However, the extent of this threat is unknown because the capability to measure and detect drone incursions is an emerging field.
- Detection technology is rapidly evolving as companies develop new products to serve expanding defense and security applications, including correctional institutions. However, many technologies are military-focused and therefore do not meet the operational needs of corrections.
- Correctional agencies may be limited by legislation such that some detection technologies are not appropriate, and interacting with drones may not be permitted under current laws unless supported by an authorized federal entity. The penal system has yet to develop a set of operational requirements to drive the development of detection technology.

Drones, or unmanned aircraft systems (UAS), delivering contraband pose a real threat to correctional facilities. Successful strategies to reduce contraband entering facilities combine technology-based solutions with associated policies and procedures. Technical complexities, legislative constraints, rules, and regulations limit correctional agencies' options when planning for the contraband threat from drones. Thus, the majority of solutions must be focused on technology-based detection to support improved facility contraband management. A variety of terms are associated with drones and are used interchangeably, but for the sake of consistency, this document uses the following definitions:[1]

- UAS: Unmanned aircraft system—an aircraft operated without direct human intervention within or on the aircraft,[2]
- sUAS: Small, unmanned aircraft system—a drone weighing less than 55 pounds on takeoff, including its load, and its associated elements (including communication links and the components that control the drone),[3] and
- C-UAS: A system or device capable of lawfully and safely disabling, disrupting, or seizing control of an unmanned aircraft or unmanned aircraft system.[4]

Drone-Delivered Contraband in Correctional Facilities

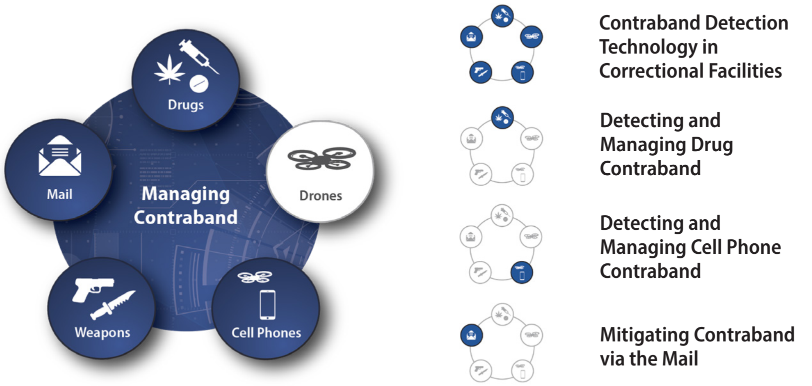

Drugs
Mail
Managing Contraband
Drones
Weapons
Cell Phones
Contraband Detection Technology in Correctional Facilities
Detecting and Managing Drug Contraband
Detecting and Managing Cell Phone Contraband
Mitigating Contraband via the Mail

Figure 1: This brief focuses on management of contraband connected to drone flyovers and drops; additional documents in this series address other contraband topics.

[1] Statutory definitions for UAS, sUAS, and C-UAS can be found at 49 USC § 44801(5), (9), and (12). Federal Aviation Administration regulatory definitions can be found in 14 CFR Part 107. Further context can be found in Department of Homeland Security and National Urban Security Technology Laboratory. (2019, September). *Counter-unmanned aircraft systems: Technology guide* (CUAS-T-G-1). Retrieved from https://www.dhs.gov/sites/default/files/publications/c-uas-tech-guide_final_28feb2020.pdf

[2] The term "aerial" may also be used to describe unmanned systems (mentioned in Department of Homeland Security and National Urban Security Technology Laboratory. (2019, September). *Counter-unmanned aircraft systems: Technology guide* (CUAS-T-G-1). Retrieved from https://www.dhs.gov/sites/default/files/publications/c-uas-tech-guide_final_28feb2020.pdf)

[3] CFR Title 14, Part 107.3.

[4] Technologies to "counter" drones may include sensors and processes for detection and mitigation that exploit the physical components of a drone and the communications between the drone and the ground control station.

Drone Threats

Drones enable varied threats to correctional facilities: threats can be either directly or indirectly related to contraband.

The three major threats to correctional facilities from drones in this regard are:

- **Smuggling Payloads**: Drones are capable of transporting/dropping contraband into correctional facilities.
- **Intentional Disruption**: Drones can be used to create a distraction to increase the chances of infiltration of contraband via other methods while security is reacting to a drone-induced incident.
- **Surveillance and Reconnaissance:** Drones can monitor an area without detection to prepare for drops.

Despite innovations and sound correctional practices, novel and inventive methods are constantly being developed and employed by persons who are incarcerated and conspirators to smuggle contraband into correctional facilities. Efforts are enabled by the constantly evolving capabilities associated with new technologies being deployed in drone designs and associated capabilities and software. For example, a recent entry to the drone market claims 120 minutes of flight time, up to 18.6 miles of range, and imaging with 4 times higher resolution than conventional HD imaging.[5]

Drones are increasingly used to drop contraband such as cell phones,[6] SIM cards, drugs, escape paraphernalia, and weapons into facilities. In fact, the Department of Justice (DOJ) stated that between 2015 and 2019 federal prisons reported 130 drone incidents; however, it is posited that this number does not accurately represent the actual threat for a variety of reasons:[7]

1. The Bureau of Prisons' (BOP's) **formal reporting policy was not established** until 2018. It is notable that after the implementation of formal reporting instructions the number of incidents recorded increased by 87%.
2. The number of drone incursions reported was **primarily based on visual observations** of drones in flight by corrections staff, which is limited by variables such as situational location, weather, time of day, and line of sight. It is important to note that most UAS flights above 400 feet are virtually undetectable by the naked eye or ear, which also strengthens the notion that the numbers cited are a significant undercount. In every case where UAS detection equipment was installed, the number of UAS flights seen in the area increased substantially.
3. **Detection technology was not employed** during the 2015–2019 UAS threat audit (e.g., radar, acoustic sensors) and therefore reinforces the assertion that the recorded incidents are well below actual events.

As illustrated by recent press about contraband being delivered via drone (see **Figure 2**), drones present a new and evolving security threat to a significant percentage of the 7,100 federal, state, local, tribal, and military prisons and jails in the United States. As a result, drone detection systems are emerging to help manage the threat of contraband to correctional facilities. Given the highly varied infrastructure of correctional facilities, ranging from high-rise incarceration facilities in the middle of metropolitan areas to isolated complexes in the middle of deserts, varied strategies are appropriate in terms of detection. However, use of these solutions, and their limitations with regard to interdiction, can be confusing. Congress has exclusively authorized the Departments of Defense (DOD), Energy (DOE), Justice, and Homeland Security (DHS) to engage in limited UAS detection and mitigation activities to counter UAS presenting a credible threat to specified facilities or assets, notwithstanding certain other applicable federal laws that relate to surveillance.[8] In addition, the Federal Aviation Administration (FAA) has been expressly authorized to engage in limited testing activities notwithstanding certain federal criminal surveillance laws.[9] However, because they have not been exempted by Congress, the same federal criminal surveillance laws may prevent, limit, or penalize state, local, tribal, and territorial and private-sector entities (including law enforcement organizations, governments, and owners and operators of critical infrastructure like correctional facilities, stadiums, outdoor entertainment venues, airports, and other key sites) from purchasing, possessing, or using UAS detection and mitigation capabilities.

[5] Advexure. (2022). *Introducing Dragonfish*. Retrieved from https://advexure.com/pages/autel-dragonfish

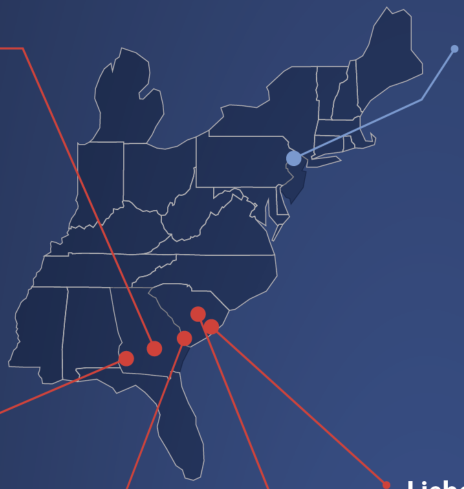
[6] Contraband cell phones can be used for escape planning, direct criminal activity outside the facility, and other nefarious purposes.

[7] Department of Justice. (2020, September). *Audit of the Department of Justice's efforts to protect Federal Bureau of Prisons facilities against threats posed by unmanned aircraft systems*. Retrieved from https://oig.justice.gov/sites/default/files/reports/20-104.pdf

[8] 10 U.S.C. § 130i, 50 U.S.C. § 2661, and 6 U.S.C. § 124n.

[9] 49 U.S.C. § 44810(g).

Recent Press on Arrests and Drone-Based Contraband



Telfair State Prison
McRae-Helena, Georgia

- Three people sentenced to federal prison time for planning to aerially smuggle contraband (including tobacco, cell phones, and a digital scale) in August 2019
- Person arrested for attempting to smuggle contraband (including marijuana, fentanyl patches, tobacco, and cell phones) in January 2022

Calhoun State Prison
Morgan, Georgia

- Three people arrested for planning to aerially smuggle contraband in February 2022
- Contraband items: 1 drone, marijuana, methamphetamine, cell phones

Ridgeland Correctional Institution
Ridgeland, South Carolina

- Person charged for planning to aerially smuggle contraband in January 2022; contraband items included a drone, marijuana, and tobacco
- Officers confiscated contraband after an attempted traffic stop where they observed a person flying a drone near the prison in July 2022 but could not locate the driver after they crashed; contraband items included a drone, marijuana, cell phones, cigarettes, cigars, cannabis flower, drone batteries, and Cash App cards

Fort Dix Federal Prison
Fort Dix, New Jersey

- Four people pled guilty to multiple drone deliveries of contraband from November 2018 to March 2020
- Contraband items: cell phones, cell phone accessories, tobacco, weight loss supplements, eyeglasses

Lieber Correctional Institute
Ridgeville, South Carolina

- Person arrested for crashing drone into prison yard in February 2022
- Contraband items: 1 drone, marijuana, tobacco, hacksaw blades, lighters

Lee Correctional Institution
Bishopville, South Carolina

- 20 people arrested for contraband operations after an 8-month investigation (May 2021 to January 2022)
- Contraband items: 12 drones, crack cocaine, knives, tobacco, guns, cell phones, candy

Figure 2: Examples of news articles that highlight recent arrests that were made because of attempts at smuggling contraband into correctional facilities via drone: red denotes incidents related to state prisons (including Telfair State Prison,[10, 11] Calhoun State Prison,[12] Lee Correctional Institution,[13] Ridgeland Correctional Institution,[14, 15] Lieber Correctional Institute[16]); blue denotes federal (Fort Dix Federal Prison[17]).

[10] Press Release, U.S. Att'y's Off. S. Dist. of Ga., Dep't of Just., *Third defendant sentenced in scheme to use drone to smuggle contraband into a Georgia state prison* (2021, August 19), https://www.justice.gov/usao-sdga/pr/third-defendant-sentenced-scheme-use-drone-smuggle-contraband-georgia-state-prison

[11] Marnin, J., (2022, January 25). Man tries to fly drugs and cellphones into prison using a drone, Georgia police say. *The News & Observer*. Retrieved from https://www.newsobserver.com/news/nation-world/national/article257713923.html

[12] WALB. (2022, February 20). *3 Arrested in Calhoun Co. prison ploy, drugs seized.* WALB News. Retrieved from https://www.walb.com/2022/02/21/3-arrested-calhoun-co-prison-ploy-drugs-seized/

[13] WLTX. (2022, February 3). *20 arrested in South Carolina prison drone-based smuggling operation.* WLTX News. Retrieved from https://www.wltx.com/article/news/crime/drone-contraband-lee-correctional-institution/101-30a58d3d-c9f6-4102-95df-e501e376ae19

[14] Murdaugh, S. (2022, January 27). Woman charged with planning to drop drugs at Ridgeland prison by drone. *Jasper County Sun Times*. Retrieved from https://www.blufftontoday.com/story/news/2022/01/27/woman-charged-planning-drop-drugs-ridgeland-prison-drone/9215840002/

[15] Murdaugh, S. (2022, August 3). Police: Drone, contraband confiscated near Ridgeland prison. *Jasper County Sun Times*. Retrieved from https://www.blufftontoday.com/story/news/2022/08/03/police-drone-contraband-confiscated-near-ridgeland-prison/10173689002/

[16] Renaud, T. (2022, March 1). *Summerville man arrested after crashing drone with contraband into prison yard*. Count on News 2. Retrieved from https://www.counton2.com/news/local-news/summerville-man-arrested-after-crashing-drone-with-contraband-into-prison-yard/

[17] U.S. Attorney's Office. District of New Jersey, Department of Justice. (2022, February 3). *Two Hudson County men admit roles in scheme to us drones to smuggle contraband into Fort Dix Federal Prison* [Press release]. Retrieved from https://www. justice.gov/usao-nj/pr/two-hudson-county-men-admit-roles-scheme-use-drones-smuggle-contraband-fort-dix-federal

The most widely reported use of drones infiltrating correctional facilities is to smuggle payloads, most often to deliver drugs, cell phones, and weapons to persons who are incarcerated.

Drone-delivered packages can range from small payloads of a few pounds to upwards of hundreds of pounds. Not all drones, however, can carry heavy payloads. Small, inexpensive consumer drones can only carry a few pounds. Drones capable of carrying heavier payloads are comparatively more expensive and have shorter flight times. Advancements in sensor deployment, control software, and object avoidance have made flying drones less difficult. Additionally, aftermarket payload release mechanisms have reduced the need to land or loiter close to the ground in order to deliver a payload.

International events, including a September 2021 incident where drone operators dropped explosives payloads over an Ecuadorian penitentiary, suggest that the use of drones for intentional disruption is an emerging trend that could surface in the United States.[18] Drones used for surveillance and reconnaissance of correctional facilities have not been reported but remain a growing concern for BOP staff.

Drone technology is constantly evolving with greater abilities to successfully deliver contraband and avoid detection.

Technology advances in drones often have made their detection and mitigation more challenging. These developments include:

- Sophisticated camera capabilities and 3D mapping software that could be used for aerial surveillance of prisons[19]
- Obstacle avoidance sensors and stability systems that enable drone operation with minimal skill
- Extended battery life, more powerful batteries, and lighter components that allow drones to fly faster and for longer periods of time
- GPS-enabled drones that can fly autonomously on predetermined flight paths using Waypoints

Human detection of drones has limitations. For example, many contraband deliveries occur in the evening hours or overnight when drones are less likely to be seen by human observers. In cases when drones are recovered by law enforcement, they have been found to be covered in tape to obscure their lights for camouflage and evade visual detection.[20] Drones can and have escaped technology-based detection and/or may be able to fly above nets.[21, 22]

Once in the facility, drone-delivered contraband can be sold for profits, leading to wider circulation of prohibited items in a single facility. The impact can be extreme, as illustrated by a situation in the Lee Correctional Institution in Bishopville, South Carolina. A conflict between rival groups in April 2021 left seven people dead and 20 injured because of the use of arms that were suspected to have entered the facility by drone. A subsequent 8-month investigation led to a "ring arrest" having proved that contraband was delivered by drone.[23]

[18] Reports of drones used for intentional disruption may involve the dropping of explosives in correctional facilities, which may result in damaging facility infrastructure. Recent incidents have not been reported in the United States but have taken place internationally as described at https://dronedj.com/2021/09/14/drones-drop-explosives-in-ecuador-prison-attack-by-suspected-drug-cartels/.

[19] Temin, T. (2020, October 19). Federal prisons are facing threats from drones dropping contraband, surveilling facilities. *Federal News Network*. Retrieved from https://federalnewsnetwork.com/agency-oversight/2020/10/ig-federal-prisons-face-danger-from-drones/

[20] "The drone, equipped with a camera and releasing mechanism, had black electrical tape covering its lights, according to the warrant." Kotowski, J. (2021, December 17). *Drone carrying cellphones crashed in Kern Valley State Prison yard: Report.* KGET.com. Retrieved from https://www.kget.com/news/crime-watch/drone-carrying-cellphones-crashed-in-kern-valley-state-prison-yard-report/

[21] "Another telling indicator of what an enormous challenge for authorities the airborne flow has become is the fact that the increasingly experienced pilots succeeded in making their deliveries despite the Lee Correctional Institution being equipped with an anti-drone detect-and-track system." Crumley, B. (2022, February 7). *South Carolina busts gangs flying contraband to prison by drone.* DroneDJ. Retrieved from https://dronedj.com/2022/02/07/south-carolina-busts-gangs-flying-contraband-to-prison-by-drone/.

[22] "These nets were put in to make these illegal deliveries more difficult, but drones can fly far above them, forcing SCDC to look for other defenses." Manion, T. (2022, January 27). *Prisons battling contraband deliveries made by drones.* WTOC 11. Retrieved from https://www.wtoc.com/2022/01/27/prisons-battling-contraband-deliveries-made-by-drones/

[23] Crumley, B. (2022, February 7). *South Carolina busts gangs flying contraband to prison by drone.* DroneDJ. https://dronedj.com/2022/02/07/south-carolina-busts-gangs-flying-contraband-to-prison- by-drone/

Managing Drones and Contraband Drops in Facilities

Managing contraband carried by drones can combine human and technical methods to detect and react to drones. Because drones are a threat to both military and critical infrastructure, numerous technologies and products are being developed and sold to detect, react to, and actively counter drones. However, the operational use case for correctional facilities differs from the battlefield, the constraints applicable to the military vary based on whether the use case is overseas or within the United States, and law enforcement officials' use of C-UAS technology faces different legal constraints than those faced by military personnel. Moreover C-UAS technology that captures, stores, and/or intercepts communication signals to or from a drone may implicate federal criminal surveillance laws. Thus, acoustic, radar, and electro-optical (EO) systems have fewer legal and regulatory restraints than radio frequency (RF)-based systems.[24]

As summarized in **Figure 3**, this brief offers high-level insights on solutions to detect and react to drones and highlights that some technologies and active[25] strategies for detecting and countering or mitigating drones present specific legal risks to agencies. When developing plans to manage drones, correctional agencies are strongly advised to review an interagency advisory published by the FAA, Federal Communications Commission (FCC), DOJ, and DHS.[24]

Drone Management for Correctional Facilities

DETECT ✓
Correctional facility security personnel as observers (both visual and audible) are recommended as part of a layered detection strategy. The goal is for observation to be established within typical patterns of duty and thus support recognition of suspicious indicators. Personnel can note the size, frame, speed, date, location, and time of observed drones, as well as where the payload is dropped and who is picking it up. More sophisticated sensor-based detection can augment human limitations to see or hear the drone at greater distances, at night, etc. Specifically, radar, optical, infrared, or acoustic sensors can be leveraged to increase the ability to locate and identify a drone; however, radio frequency (RF)-based detection may present legal issues.

REACT ✓
Once a drone is detected, facility staff need to consider the threat from that drone, including if a drop has occurred. If a drop is confirmed the next actions are to intercept/confiscate the contraband and identify the recipient(s). Where appropriate, flight data, pilot location, or identification can be determined and used to take legal action. As such, facilities need staff who are available and trained on how to respond. Law enforcement may also be involved, especially where drones and drops are found outside the correctional facility.

ACTIVELY COUNTER ?
Simple countering options exist in the form of physical barriers like nets, which are appropriate for any facility; however, many technology-based active countering solutions are not. When implementing sophisticated active countering strategies (i.e., deter/neutralize, interfere/interdict, or negate/destroy), legislation and policies may limit options and actions. Technical methods to actively counter drones present legal challenges for entities other than federal agencies like DHS, DOJ, DOD, or DOE. For any counter-drone planning effort, specific rules on use of force need to be clearly identified/defined, and systems and processes need to align with legislative and policy limitations specific to the facility.

Figure 3: Drone-delivered contraband can be managed with careful design and implementation of technology, policies, and practices, whereas countermeasures may create legal issues.

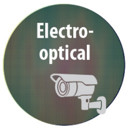
[24] Department of Justice. (2020, August). *Advisory on the applications of federal laws to the acquisition and use of technology to detect and mitigate unmanned aircraft systems*. Retrieved from https://www.justice.gov/file/1304841/download

[25] Passive management reduces the threat of a drone without disrupting it (e.g., blocking view, locking cells/gates, searching for drops), whereas active measures physically stop the detected drone using jamming, spoofing, electromagnetic pulse, laser, etc.

DETECT: Best practices for drone detection combine multiple technology approaches within an operational system that includes well-trained staff.

Detection of drones can be by staff directly seeing or hearing the drone or by using various technologies (e.g., acoustic, optical, RF) to sense or detect the drone. Corrections personnel are an important part of the operational system to manage drones and contraband drops; they can monitor the airspace around a facility, as well as locate and track drones and operators to enable the facility to react (see **Figure 4**). Technology-based systems can help staff by combining multiple methods of detection to create a system-level approach. Common technologies used for drone detection include:[26]

Radar systems use radio waves to detect and track airborne threats. The advantages of radar include coverage of large areas, tracking of multiple objects in most weather conditions, and the ability to detect drones that are programmed to "run dark."[27] Limitations include a higher amount of nuisance alarms due to birds and obstructed views at lower altitudes. Newer systems can be configured to alert when objects are deemed to be a drone by using machine learning and artificial intelligence (AI) to help reduce false positives. Newer micro-Doppler radar can detect the movements of small rotors on drones.[28]



Electro-optical (EO) systems use camera and video-based detection to "see" drones. They can record the intruding drone; however, these systems are limited in their field of view, which can be negatively affected by trees, structures, weather, and darkness. Analytics aimed at detection of both objects and motion improve system performance, but an unobstructed line of sight is always required to detect objects. Both visual and infrared (IR) detection systems are used.

Acoustic systems use microphones to detect noise signals that are processed to determine if a drone is in the area. The tracking ability of acoustic systems is reliable and accurate but is limited to shorter distances than some of the other technologies, and noisy environments may present additional challenges. Acoustic systems provide basic initial information about the location and direction in which a drone is traveling.

Radio frequency (RF) systems use antennas to detect communications between a drone and its controlling device. These systems can typically detect drones at distances of up to 20 miles and can even reach limits of up to 100 miles given perfect meteorological and terrain conditions. However, they can only detect within certain frequency ranges. If the drone operates outside of those frequencies or is autonomous, the drone will not be detected. RF-based detection may present legal risks to agencies.

The four detection technologies introduced above (radar, optical/visual, acoustic, and RF signals) are enabling emerging products for detecting drones at correctional institutions. Each technology type presents strengths and weaknesses that must be properly vetted for specific operational use cases. Environmental and infrastructure considerations and other causes of potential interference, such as RF and ambient noise levels and aerial/vehicle traffic, must also be considered. Furthermore, RF signal detection platforms may present legal challenges, and before purchasing or operating them, agencies should review the interagency advisory and consult with legal counsel to ensure compliance with all federal and state laws. Ultimately, the best approach to drone detection may be a combination of technologies that are complementary to each other.

[26] Derived from Baker, S. (2020, May 26). *How correctional facilities can use drone detection tech to stop contraband delivery*. Stanley Security. Retrieved from https://www.stanleysecurity.com/blog/how-correctional-facilities-can-use-drone-detection-tech-stop-contraband-delivery

[27] Radar can be used to detect drones that are not emitting or receiving an RF signal.

[28] Radar systems should be coordinated with the FAA prior to use.

Historically, technology development is often driven by the military markets and DHS's active exploration of drone detection for protection of critical infrastructure and nondefense applications within U.S. borders. These efforts are still nascent and highly fragmented in terms of applications, technologies, products, and suppliers. As an example of a relevant use of C-UAS technology to protect infrastructure, a detection system is being designed to protect a nuclear power plant using radar detection; this example covers an area similar to what might be needed for a correctional facility. Hardware and installation costs for the four radar stations needed are on the order of $200,000. Design, implementation, and operational changes would result in additional costs.[29]

Drone detection systems may be able to (1) sense the presence and location of a drone,[30] including, in some cases, altitude, speed, and drone make/model/ID, as well as (2) detect and track drone pilot location and movement. These systems can help provide warnings and alerts to enable reaction by personnel and capture and retain information about the drone intrusion as evidence in any future legal cases.

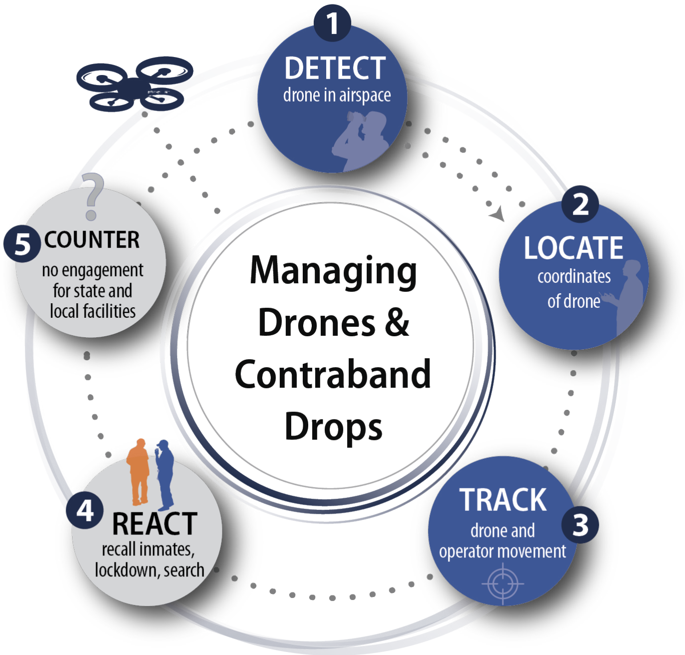

Managing Drones & Contraband Drops
1 DETECT drone in airspace
2 LOCATE coordinates of drone
3 TRACK drone and operator movement
4 REACT recall inmates, lockdown, search
5 COUNTER no engagement for state and local facilities

Figure 4: Products and services can help facilities assess drone threats and implement systems to detect, locate, and track drones and operators to enable an operational response within the facility and with local law enforcement.

Examples of drone detection products currently used at correctional facilities are provided on the next page. These selected products highlight solutions on the market and the technologies being used; the list is illustrative not exhaustive. Some of these are used at federal facilities that have different legal capacities to use technology associated with drone management (e.g., express exemptions from certain federal criminal surveillance laws) and would NOT be appropriate for state and local facilities today. Many of the companies discussed are global and also offer mitigation solutions for correctional facilities that may be legal in other countries but may not be broadly legal in the United States. They were selected to illustrate the kinds of products and services available to correctional facilities. This list is NOT exhaustive, nor does CJTEC or NIJ recommend or provide any opinion on these companies or products. Beyond these products, several rural facilities shared with CJTEC that they use less expensive trail/game cameras beyond their perimeter. In one case, they used a connected system, where the camera signal was available in real time at the facility. At another, they used cameras for which data cards needed to be retrieved. These facilities used the cameras to build evidence of drone operators who were surveilling the correctional facilities, testing their systems, and attempting to deliver contraband.

[29] Coggin, J., & Jones, T. (2021, April 28). Personal communication.

[30] Yaacoub, J-P., Noura, H., Salman,O., & Chehab, A. (2020). Security analysis of drones systems: Attacks, limitations, and recommendations. Internet of Things, 11, 100218. http:/doi.org/10.1016/j.iot.2020.100218

Example Drone Management Products and Companies

The following list is illustrative and does not represent an endorsement or confirmation of the capabilities of any company or product by NIJ or CJTEC.

- Aerial Armor, located in Arizona, offers mobile drone detection for law enforcement and integrated systems for facilities. It is representative of companies that provide drone detection services in a layered system using various equipment and supporting software. Its website states that the company typically recommends DJI AeroScope (cyber-hardened) for RF signal interception (see below), radar, optical technology (thermal cameras), software, and mitigation (where appropriate).

- AeroScope, from DJI (global drone market leader in China), uses drone communication protocols to understand flight status, paths, and other information in real time to inform a response. It can identify most DJI drones in the market today by analyzing their electronic signals. It is distributed by numerous U.S. companies, including some on this list, like 911 Security (below) and Aerial Armor (above). Because of unique factual and legal circumstances, despite reliance on RF-based signals collection, the AeroScope product can lawfully be used by agencies without an express exemption from federal criminal surveillance laws, which enables law enforcement to legally track and detect ground controllers and UAS.

- AirGuard, from 911 Security, headquartered in Texas, uses an array of sensors, including RF detection and video, to track drone flights and locate drone pilots and claims to be able to integrate with existing security infrastructure such as alarms, video cameras, and access control at correctional facilities.

- AirWarden, from AeroDefense, claims to be able to detect drones often before they take flight to locate the drone's controller. The system can be procured in either a fixed, portable, or vehicle-mounted platform. The company claims a state prison system is using AirWarden to detect drones to alert staff and react via lockdown within minutes; staff have confiscated contraband, including tobacco and cell phones and, although they note the associated difficulty, have caught drone operators. The company is a U.S.-based woman-owned small business with their development team based in New Jersey.

- Dedrone, with business operations in the United States, United Kingdom, and Germany, claims to be used at more than 50 correctional facilities globally. Dedrone offers a process where facilities first diagnose their airspace activity and use this information to build a threat profile. They claim a state department of corrections has deployed the Dedrone RF-100 and was able to see actionable drone activity data, including times, dates, and types of drones entering their airspace. Dedrone has also been used by the Kentucky Department of Corrections to help alert their facilities to drones within 1 mile to initiate their scanning procedures. The awareness of drones after dark has been of value because it is illegal for hobbyists to fly drones after dark.[19]

- DroneDefence is a U.K.-based company with products focused on specific drone-centric needs and integrated systems. Example products include Aerosentry, which uses RF technology to detect drones; Aeroeye, which uses fixed focal length scan cameras and AI-enabled video analytics; Aerosense, which uses radar for mobile and rapid deployments; and other products to counter or defeat drones.

- EnforceAir, from D-Fend Solutions, is a C-UAS product that likely is only appropriate for federal use because of the focus on mitigation. The system claims to detect unauthorized drones (not the facilities' drones), identify them, and then automatically take control over the drones and land them in a safe, designated area. The product is designed to provide prison authorities with data related to drone takeoff position and pilot remote control location to help police apprehend the perpetrators and prevent future intrusions.

- GroundAware is Observation Without Limits'(aka OWL—headquartered in Alabama) radar-based surveillance solutions using digital radar technology. It is a perimeter security system designed to detect intrusion broadly, not just drones. GroundAware's digital beam-forming radar technology continuously monitors for threats in low-altitude airspace to detect, classify, and track drones. OWL has stated it is working on integrated radar/camera systems "at the first of up to six corrections facilities in the southeastern United States. Officials at these prisons made the decision to go with long-range radar after a pilot project in which the technology was field-tested and proven to provide the situational awareness needed to protect perimeters on the ground and in the air."[20]

- Sheltron, with business operations in the United States and Colombia, offers both drones and UAVs, as well as counter-drone and other security services and products. They claim to offer both fixed and mobile systems for correctional facilities with the ability to purchase or lease the system.

- SkyDome, from Fortem Technologies, claims to monitor a facility's airspace with their TrueView radar, which then assesses the danger and alerts security professionals of intrusions. SkyDome uses AI to create a network mesh to protect the airspace and integrates with other security and, for legally appropriate facilities, enables mitigation. Because it is a radar-based system, it can detect drones that have been programmed to "run silent." Based in Utah, the company is privately held and backed by Toshiba, Boeing, and other venture partners.

- SKYLOCK is an Israeli company that offers correctional facilities a C-UAS platform that detects and mitigates unauthorized drones with 360° coverage using EO/IR acquisition, RF, and radar detection.

[31] Vimeo. (n.d.). *Stopping drone contraband at Kentucky Department of Corrections* [Video]. Retrieved from https://vimeo.com/535895976

[32] CN Staff. (2021, October 14). Newly developed tech addresses today's drone threat. *Correctional News*. Retrieved from https://correctionalnews.com/2021/10/14/newly-developed-tech-addresses-todays-drone-threat/

REACT: Best practices use technology and policies to react at the facility, to apprehend the operator, and to inform associated investigations.

Facilities that have detection systems, trained staff, and agreements with law enforcement partners are better positioned to (1) reduce the influx of contraband and the associated issues it creates, including threats to staff and inmate safety; (2) detect and apprehend the ground-based controller and operator; and (3) build evidence to convict perpetrators.

FACILITY

Upon detection of dropped contraband, the facility must have trained staff and policies to "render safe" the situation. Although bomb squads are recommended, timing is challenging because staff need to react to the situation. The staff will need to recall inmates, lock down the facility, do area searches, and know how to maintain safety and protect evidence. A significant variable for success is the investment and hard work needed to be prepared. This can include acquiring technology and putting into place policies, protocols, and formal agreements with local law enforcement to specify authorities and responsibilities for a quick response beyond the facility.

OPERATOR

Some technologies that have been discussed can detect and track the ground controller; however, this is not the only way to locate and apprehend the operator. Facilities have used trail/game cameras at strategic locations to gain information on developing threats and coordinated with local law enforcement to successfully apprehended drone pilots.[33,34] Also, contraband cell phones have been confiscated that provided information on drone runs and drops.

EVIDENCE

With proper strategy and investigations, significant evidence can be captured and leveraged for successful prosecution. In one case, facility CCTV captured a drone dropping a laundry bag that appeared to be from the facility on top of a pile of facility laundry bags and an inmate retrieving that bag. When either contraband or drones are recovered by corrections officials or law enforcement, connection to forensic laboratories, especially those that specialize in digital forensic services, is important. As described below, beyond traditional forensic evidence like latent prints, the operational elements of drones and cell phones delivered by drone can provide important information on the drone's purchase, operations, flight patterns, and locations.

DRONES and COMPONENTS OFFER SIGNIFICANT INSIGHT ON THEIR USE AND USERS

Drones consist of the flight portion (i.e., motors, airframe, battery, power source) but are enabled by the onboard sensor suite, data collection system, and processing power. The onboard sensor suite, data collection system, and processing power gather and store valuable data. Understanding this is vital when assessing the value of forensic evidence on a captured drone or its controller (which itself is often a smartphone or rudimentary computer). Law enforcement and corrections officials must comply with controlling legal authority, including the need to obtain proper legal process (e.g., a search warrant) before forensically exploiting a drone or its associated data. However, the data that can be retrieved, and insights to be gained, from a legally authorized forensic analysis of a drone are extraordinary. The data do not merely provide information such as captured video or flight paths, but also a vast array of insights and raw data. Depending on the UAS and method of analysis employed, such data may include:

- Evidence and indications of operations since initial activation
- Email addresses of the user
- Audio recordings and commentary before, during, and after operation
- Verification of deployment of payloads
- Operator's home, work, and practice locations
- Identification of other drones that components (such as batteries) may have been used in, thereby developing a network model
- Other individuals involved based on determining other controllers used with the subject drone
- More conventional forensic physical data and information made easier to obtain by the myriad of serial numbers, environmental data, and information stored in almost every component of a drone

[33] Roberts, B. (2022, April 19). Personal communication.

[34] Galloway, T. (2022, March 16). Personal communication.

COUNTER: U.S. state and local facilities have limited options to engage with drones.

C-UAS solutions are of great interest today broadly, most of which have been developed for military and defense purposes. As discussed previously, different systems and technologies are being matured to meet complex threat and operational scenarios for global military, border, justice, infrastructure, event, and commercial needs. These systems are often complex and expensive.[35] Nondefense applications within U.S. borders are only at the early stages of development and deployment broadly. Application is limited by performance challenges, practicality, and, most importantly, safety and legal considerations when the technologies and operation of systems are aimed at countering drones within U.S. civilian areas. Capabilities for detecting and mitigating drones may implicate federal criminal laws, including those relating to surveillance, access and damage to computers, and damage to an aircraft. U.S.-based corrections officials contemplating testing, acquisition, installation, or use of UAS detection or mitigation systems should seek the advice of counsel and are strongly urged to consult the Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems. The advisory discusses the interplay of federal laws and regulations on C-UAS operations and how they may affect contemplated use of C-UAS technology.[36]

Outside the United States, some counter-drone systems are being proven to help reduce the incidence of drone-delivered contraband and are gaining acceptance for prison use. One example is the 6-month experiment in England, which "prompted ministers to consider a U-turn about the technology. Prison governors and officers and the chief inspector of prisons have expressed frustration at the failure of HM Prison Service to use technology to prevent drone smuggling fueling the growing drug problem in jails." In the United Kingdom, prisons have the legal authority to block cell phone signals, and the authorities in Guernsey amended the legislation to include drones. The system tested during this evaluation blocked transmission signals, which resulted in the drone's homing system returning the unit to its operator without damage, thus keeping the prison from having issues with errant civilian drones.[37]

LEGAL and POLICY CONSIDERATIONS

In 2018, Congress passed the Preventing Emerging Threats Act of 2018, as part of the Federal Aviation Administration Reauthorization Act, which exclusively authorizes the Departments of Defense, Energy, Justice, and Homeland Security to engage in limited UAS detection and mitigation activities, notwithstanding certain otherwise potentially applicable federal laws. Because no other entities have been granted that authority, it is important that correctional leadership at nonfederal levels understand that federal laws and regulations may prevent, limit, or penalize the sale, possession, or use of C-UAS technology. Jamming or emitting technology cannot be legally sold by C-UAS vendors without approval from the FCC. Prior to installation and use of C-UAS in correctional facilities, correctional executives should conduct a legal analysis of the C-UAS functional capabilities to avoid violation of federal laws. Detection and mitigation capabilities of C-UAS may violate federal regulations relating to surveillance, access and damage to computers, and destruction of aircraft. These technologies may also implicate federal laws and regulations relating to aviation security and use of the RF spectrum. Correctional leaders can refer to the DOJ Advisory on C-UAS technologies.[38]

[35] As illustrated by the U.S. Air Force awarding Leidos a $27M contract to build a prototype of an antidrone system using "first-generation high-powered microwave" for airbase defense. The system provides nonkinetic defeat of multiple drones. Unmanned Airspace. (2022, March 1). *Leidos awarded USD 27 million DoD contract for high power microwave C-UAS prototype*. Retrieved from https://www.unmannedairspace.info/counter-uas-systems-and-policies/leidos-awarded-usd27-million-dod-contract-for-high-power-microwave-c-uas-prototype/

[36] Department of Justice. (2020, August). *Advisory on the application of federal laws to the acquisition and use of technology to detect and mitigate unmanned aircraft systems, guidance document #9.95.300-UAS*. Retrieved from https://www.justice.gov/jm/9-95000-unmanned-aircraft-systems-uas#9-95.300

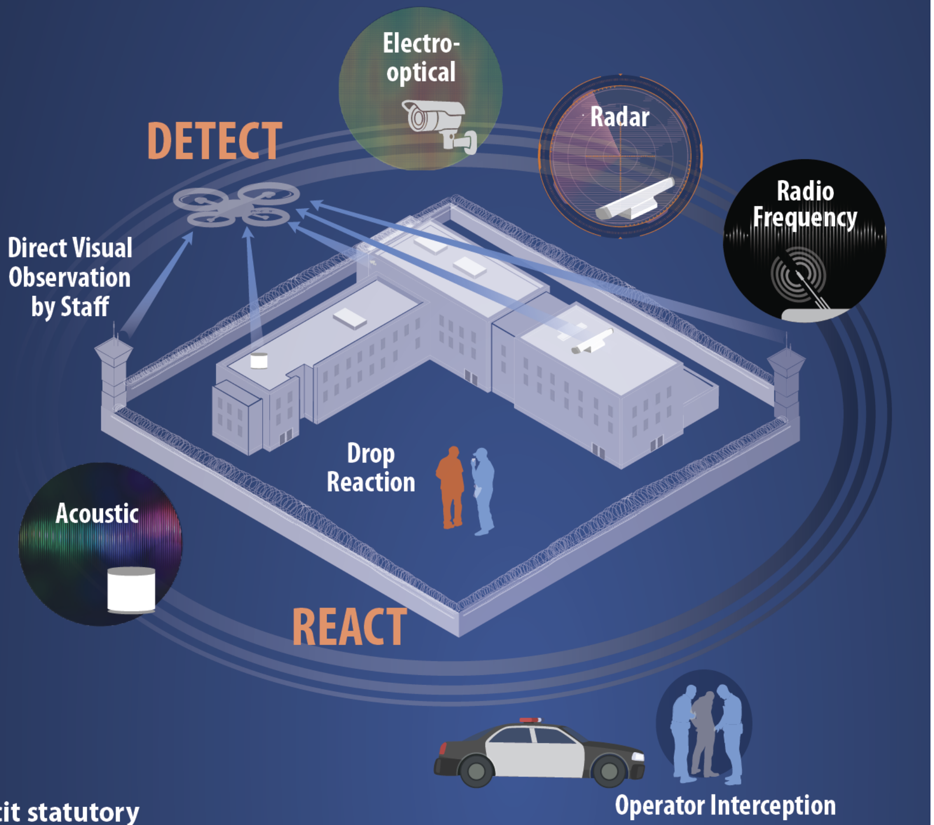
[37] Weaver, M. (2018, December 18). Anti-drone technology could be introduced in English prisons. *The Guardian*. Retrieved from https://www.theguardian.com/society/2018/dec/18/anti-drone-technology-introduced-english-prisons-skyfence

[38] FAA Reauthorization Act of 2018, H.R. 302, 115th Congress. (2018). Retrieved from https://www.congress.gov/bill/115th-congress/house-bill/302/

Key Considerations for Leaders in the Corrections Community

Drone Detection and Response

To reduce contraband that enters by drone, a facility must be able to detect the drone and counter it using legal methods, such as intercepting the operator and reacting to the drop. Detection by radar, electro-optical, and acoustical methods may be permissible under federal law. Radio frequency detection methods may be permissible, but federal laws are complex. Regardless of detection, any type of direct interaction with a drone (i.e., control, capture, or destruction) presents specific legal risks to agencies.



Systems that do not require explicit statutory authorization are available that offer potential detection solutions to the threats posed by drone flyovers. Layered detection strategies are preferred over singular methods, which are not broadly effective. However, layered strategies can be complex, expensive, and still may be well less than 100% effective. Detection and surveillance solutions are complicated by performance limitations related to placement, including terrain (e.g., line of sight), interference (e.g., noise), and safety (e.g., over roads).

Implementation of C-UAS strategies must work within federal, state, and local laws and regulations that govern detection and mitigation related to aviation safety and efficiency, transportation and airport security, and RF signals. Existing security procedures and policies of the correctional agency must be considered when designing and implementing solutions to avoid legal and compatibility issues.

Figure 5: Layered detection strategies, as well as operational policies and procedures for facility staff, in conjunction with local law enforcement can help facilities reduce the impact of drone-delivered contraband.

Key Questions to Ask

Challenges	Key Questions to Consider
Policy and Legislative Constraints	□ Have you considered and sought legal guidance on operation of the system? □ If implementing a radar-transmitting device, do you have approval from the FCC?
Operational Achievability	□ Do you understand the level of drone events; have you done a threat assessment to identify the hierarchy of current and anticipated drone incidents, the potential and specific detection technology, and deployment options that are consistent with applicable laws and agency regulations? □ Have you performed a drone risk assessment to evaluate infrastructure, location and geography, current operational capabilities, staffing and resources, and security doctrine? □ Have you considered how a technology-based detection system will affect or interface with reaction processes and security systems, policies, and reporting protocols? □ If ready to procure a system, how versatile is the system in fitting facility constraints (e.g., space, power)? □ How much investment is required related to training to operate the new system in accordance with specifications (i.e., validation, documentation, manuals, drawings) and to react to drone threats and drops (i.e., protocols)? □ Do you have what is needed to install the system in the facility infrastructure (that can be confirmed to fit within operational doctrine) and to maintain it to the required level? □ What is the available budget? Would low-cost solutions (e.g., netting, trail/game cameras) suffice? □ What costs are associated with purchasing or leasing and operating and maintaining the system?
Other Considerations	□ Are there health risks associated with the device, and if so, what mitigation strategies are needed to reduce them? □ Does the adoption of the system create personnel issues? □ Is there risk of malicious use of the system? □ Do you have forensics support that is sophisticated in recovering information and evidence from drones? □ Do you have systems to trigger periodic assessments of the system, policies, procedures, and practices to evaluate impact and adjust based on metrics associated with both current and emerging threats?

Published: **October 2022**

More Information

Steven Schuetz
Senior Science Advisor/Physical Scientist
National Institute of Justice
U.S. Department of Justice
Steven.Schuetz@usdoj.gov
Tel +1-202-514-7663

Jeri D. Ropero-Miller, PhD, F-ABFT
Project Director, CJTEC
RTI International
jerimiller@rti.org
Tel +1-919-485-5685

Jim Redden
Innovation Advisor
RTI International
jredden@rti.org
Tel +1-919-248-4222

Suggested Citation

Dix, M. O., Mecray, M., Man, J., Vetter, E., Tucker, M., Parsons, N., Craig, T., & Criminal Justice Testing and Evaluation Consortium. (2022). *Contraband and drones in correctional facilities.* Research Triangle Park, NC: RTI International.

CJTEC would like to thank Tombo Jones, Director, and John M. Coggin, Chief Engineer, Virginia Tech, Mid-Atlantic Aviation Partnership; Mark Greene, Supervisory Program Manager/ Div. Director, NIJ; Kevin Jinks, Sr. Counsel, DOJ; Tyler Galloway, Asst. Project Manager, Div. of Security, SCDOC; Sheriff Brian K. Roberts, Brunswick County, VA; and Maria Ashbaugh, Sharon Barrell, Kristina Cooley, and Rebecca Shute, RTI International, for their expertise and insights in developing this document.

This publication was made possible by Award Number 2018-75-CX-K003, awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect those of the Department of Justice.

http://cjtec.org/