NIJ UPDATE

Addressing contraband in prisons and jails as the threat of drone deliveries grows

By National Institute of Justice Staff

istock/evandrorigon

The opinions, findings, conclusions, and recommendations expressed in this publication do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Every day, correctional facilities face formidable threats from contraband such as illicit weapons, drugs, and cell phones. Prison and jail leaders and staff need new, more sophisticated means of stopping and seizing contraband before it reaches a facility's population. One concern is the growing capabilities of drones that can deliver contraband into a facility.

To help correctional leaders make the right decisions to slow or stop the flow of contraband, the National Institute of Justice has created a series of reports that identifies and assesses an array of contraband risks and reviews technologies and strategies to address them. These reports were developed by NIJ's Criminal Justice Testing and Evaluation Consortium. (Learn more about the consortium at cjtec.org).

The reports offer foundational insights from use cases, highlight challenges of contraband detection, compare illustrative products, and discuss the future of contraband detection and management.

The five reports on contraband are:

1. Contraband and Drones in Correctional Facilities
2. Contraband Detection Technology in Correctional Facilities
3. Detecting and Managing Drug Contraband
4. Mitigating Contraband via the Mail
5. Detecting and Managing Cell Phone Contraband

Download each brief at https://cjtec.org/technology-foraging/contraband-detection-management.

Figure 1

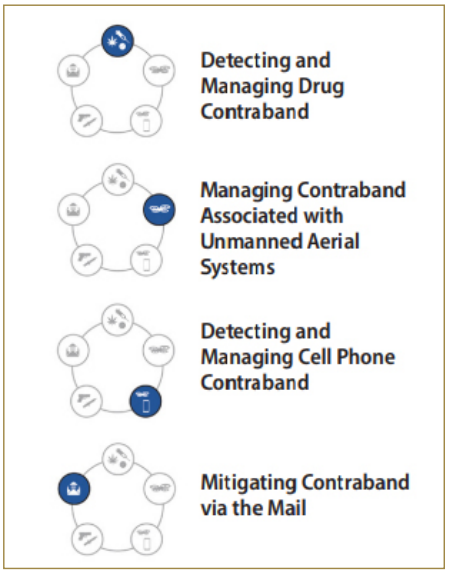

Figure 1: Contraband detection must consider methods of entry, types of contraband, and other associated factors. Reports in this series highlight technologies used and their associated trade-offs related to performance, price, and operational issues.

This article focuses particularly on contraband and drones; however, it's important to mention the following key takeaways from the other four reports.

Contraband detection technologies in correctional facilities:

- Contraband detection technologies scan for contraband that is either carried by or on a person, in a vehicle, or within an environment or space.
- Handheld devices designed to detect contraband on a person are low cost, portable, and effective but take more time to scan.
- Walk-through devices speed up scanning but are more expensive.
- Less expensive detection options are limited in the types of contraband that they can detect.
- More expensive options can detect more types of contraband than less expensive options; however, more expensive options may have higher radiation exposure than options that are less expensive.
- Handheld devices that detect vehicle-borne contraband are less expensive than drive-through detectors but have limited range and require more scanning time.
- Environmental detection technologies can identify contraband hidden in walls, furniture, mail, and packages. These portable and fixed devices vary widely in their range, cost, and ability to detect various types of contraband.

Detecting and managing drug contraband:

- Strategies that focus on drug detection at the points of entry to the facility have the greatest potential to mitigate drug contraband.
- Eradicating drugs from the prison system requires a comprehensive and multimodal approach.
- A multi-layered detection approach using X-ray scanners, chemical detection devices, digitized mail programs, and facility-based drug treatment programs can significantly reduce drugs within correctional facilities.
- Drugs are commonly smuggled into prisons and jails by incarcerated persons, staff, and visitors. Concealment efforts make it difficult to identify incoming drugs with any one technology or strategy.
- Technology can address challenges presented by variations in drug composition and drug smuggling routes, but technology cannot fully replace corrections staff assigned to identify and seize contraband.
- It is critical to engage the community because awareness of drug interception strategies may deter attempted drug smuggling and recidivism.

Mitigating contraband via the mail:

- Digitizing the incoming personal mail of incarcerated persons may reduce the flow of drugs into facilities.
- Drugs cannot be smuggled in regular mail when all mail is diverted to an offsite mail processing vendor that digitizes the written content.
- The shutdown of the mailroom pipeline will not reduce the demand for drugs by incarcerated persons. Pressure on other common contraband pathways (for example, smuggling by staff and visitors, "throw-overs," or drone drops) could increase if mail is digitized.
- When implemented as part of a bundled communications platform serving incarcerated persons and coordinated to take advantage of the need for fewer

mailroom staff, digitized mail can be cost-efficient.

Detecting and managing cell phone contraband:

- Cell phone technology advances continuously and makes detection and deterrence a challenge.
- A multilayered system of defense in a correctional facility can systematically defend against the flow and use of cell phone contraband.
- Detection technology, such as radio frequency detection, that can locate a cell phone signal or recognize components that are trafficked at multiple locations within a facility shows the greatest promise for limiting cell phone contraband.
- New technologies, such as micro-jamming and managed access systems, can disrupt and disable cell phone signals, but they have significant disadvantages. They can conflict with federal policies, they are costly, and targeted phones may still function with Wi-Fi or other communication methods.
- SIM card exchanges are increasingly used as a means of communication that circumvents the need for cellular communication. Currently, no technologies comprehensively disable SIM cards. Existing technologies in this space work well in theory but often have limitations when applied to the real-world setting of a high-security correctional facility.
- Corrections leaders must deploy technologies to deter contraband cell phone use that fit their agency operational use case. For smaller facilities, mass shakedowns of housing units and recreation areas using metal detectors or systems that detect magnetic objects may sufficiently deter forbidden cell phone usage.

"The most promising strategy against illicit drone activity is a multilayered approach that merges sensor capabilities to overcome the performance gaps of an individual technology."

— Neal Parsons

A closer look at drones and contraband

As the specter of drones delivering contraband grows so does the need for new technology to detect illicit drone flights and apprehend drone operators.

Research by NIJ's Criminal Justice Testing and Evaluation Consortium offers new insights on:

- The growth, and growing sophistication, of drone technology.
- The multi-faceted threat drones pose to the correctional system.
- Rapidly evolving technology to detect drones.
- Key policy and practice considerations for leaders of correctional facilities and systems.

Actual and perceived legal constraints on detection tools stand in the way of progress on the deployment of drone detection technology. Capabilities for detecting and mitigating drones may implicate federal criminal laws, including those related to the surveillance of, access to, and damage to computers and damage to aircraft. Further, the rapid sophistication of drone technology challenges developers to keep up with current trends.

Efforts to defeat drones that carry contraband face additional barriers, including:

- Uncertainty about the extent of the threat posed by drones because our ability to measure drone capabilities is still emerging.
- Many current detection technologies are military-oriented and may not fit the operational needs, budgets, and restraints of the corrections field. (For example, to date, it has not been a requirement or standard practice for a correctional facility to have a manager of air domain awareness and countermeasures.)
- The penal system has not yet developed operations standards to guide drone detection and abatement.

"No one drone detection technology is a panacea; they all have their strengths and limitations," said Neal Parsons, a research forensic scientist with the Criminal Justice Testing and Evaluation Consortium. "The most promising strategy against illicit drone activity is a multilayered approach that merges sensor capabilities to overcome the performance gaps of an individual technology. This is especially important given the high variability in drone designs and functionality."

istock/BehindTheLens

The evolution of technology

Correctional staff tasked with identifying and responding to drones must overcome technology that is quickly gaining enhanced abilities to deliver contraband and avoid detection.

Advances in drone technology have made detection and mitigation more challenging. They include:

- Sophisticated cameras and 3D mapping software that could be used for aerial surveillance of prisons.
- Obstacle avoidance sensors and stability systems that make drones easier to operate with minimal skill.
- Better batteries and lighter components that enable drones to fly faster and longer. (One new drone design claims to have 120 minutes of flight time and a range of up to 18.6 miles.)
- The ability to fly autonomously on predetermined paths.

Several detection technologies can augment human observation of drones in a corrections environment and may help us gain a better understanding of the scope of the threat posed by drones. But some technology designed to counter drones by capturing, storing, or intercepting signals to or from a drone may violate federal communications laws. Luckily, acoustic, radar, and electro-optical systems have fewer legal restraints.

Newer drone detection technologies have greater detection perimeters than older systems. Other promising technologies, for example the use of microphones that can detect drone blades, are also being developed.

No good measure of the drone threat

Between 2015 and 2019, the Department of Justice reported 130 drone incidents in federal prisons, but that count is almost certainly low. The Federal Bureau of Prisons did not adopt a formal reporting policy until 2018. (After reporting instructions went into effect, the number of incidents recorded increased by 87%.)

Conventional drone counts also rely on visual observation, usually by corrections staff. Such observations are limited and are affected by time of day, line of sight, weather, and drone altitude. However, most smaller drones flying above 400 feet are virtually undetectable by the human eye. Notably, in every instance when a facility installed drone detection equipment, sightings of drone flights increased substantially.

Drone detection and response: A combination of staff and technology

The contraband and drones report discusses three approaches to address the threat that drones pose to a correctional facility:

Detect. Correctional security staff serve as visual and audible observers. The report recommends that security staff serve as part of a layered drone detection strategy. More sophisticated, sensor-based detection can supplement human observers by use of sight or sound to identify drones at greater distances, subject to legal limitations.

React. When a facility detects a drone, staff must assess the threat and determine whether and where a

contraband drop has occurred. The next step is to intercept and confiscate the contraband and identify the recipient. Where appropriate, flight data, pilot location, or identification can be assessed and used to support legal actions. Facilities need staff trained to respond to drones.

Actively counter. The Consortium strongly advises correctional agencies that develop drone management plans to consult an interagency advisory published by the Federal Aviation Administration, the Federal Communications Commission, the U.S. Department of Justice, and the U.S. Department of Homeland Security.

Dealing with drones and contraband: General considerations and questions

The report identified key policy and practice considerations:

1. To reduce contraband that enters by drone, a facility must be able to detect the drone and counter it by legal methods. Radio frequency detection may be permissible, but federal laws are complex. Direct physical interaction (that is, control, capture, or destruction) with a drone presents specific legal risks to agencies.
2. Drone detection systems that do not require explicit authorization (as mandated by statute) offer greater detection solutions to drone flyovers than those that do require authorization.
3. Facility strategies to stop drones must be compatible with federal, state, and local laws and regulations related to aviation safety and efficiency, transportation and airport security, and radio frequency signals as they apply to drones.
4. Layered detection strategies are more likely to be effective, but still can be complex, costly, and less than 100% effective.

The following are standard questions for correctional leaders when considering drone detection technology.

Policy and legislative constraints:

- Have you considered and sought legal guidance on how to operate the system?
- If implementing a radar-transmitting device, do you have approval from the Federal Communications Commission?

Operational achievability:

- Do you understand the level of drone events?
- Have you completed a threat assessment to identify the hierarchy of current and anticipated drone incidents, the potential and specific detection technology, and deployment

DRONE DETECTION TECHNOLOGIES

RADAR systems use radio waves to detect and track drones. Advantages of radar include large area coverage; multiple objects tracking capability; and tracking of drones designed to avoid visual detection.

ELECTRO-OPTICAL systems use camera and video detection (both visual and infrared) to see drones, aided by analytics that assist detection of objects and motion. These systems depend on an unobstructed sight line.

ACOUSTIC systems detect noise signals that are processed to determine whether a drone is in the area.

RADIO FREQUENCY systems use antennas to detect communications between a drone and its controlling devices. They can detect drones from miles away but can only detect drone communications within limited frequency ranges. A drone that operates outside of those ranges, or autonomously, cannot be detected. These systems may present legal risks to agencies.

Radar: istock/Turac Novruzova; Optical: istock/Ali Kahfi; Acoustic: istock/Mariyall; Radio: istock/bgblue

istock/helivideo

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 the facility is ready to procure a system, how will the system fit within facility constraints (for example, space, power, and environment)?
- How much time or money is required to train operators of the new system in accordance with specifications and to react to drone threats and drops?
- Does the institution have what it needs to install the system in the facility infrastructure that fits within the operational doctrine and to maintain it to the required level?

Budget:

- Would low-cost solutions, such as netting or trail or game cameras, suffice? Do you include cost of monitoring the cameras in total cost?
- What costs are associated with purchasing or leasing, operating, and maintaining the system?

Other considerations:

- Are health risks associated with the detection device? If so, what mitigation strategies could reduce them?
- Would adopting the system create personnel issues?
- Is there risk of malicious or unlawful use of the system?
- Do you have sophisticated forensics support to help lawfully recover information and evidence from drones?
- Do you have measures to trigger periodic assessments of the system, policies, procedures, and practices to evaluate impact and adjust to both current and emerging threats?

Other resources

Of course, drones are not the only type of contraband carrier that policymakers and practitioners should consider. To learn more about dealing with contraband in correctional facilities, review the reports from NIJ's Criminal Justice Testing and Evaluation Consortium, which are available for download at https://cjtec.org/technology-foraging/contraband-detection-management/.

Here are some important resources that you should consider when looking into the detection and mitigation of drones used to bring contraband into a facility:

- Fact Sheet: The Domestic Counter-Unmanned Aircraft Systems National Action Plan, The White House (April 25, 2022).
- Justice Department Issues Statement on the Administration's Counter Unmanned Aircraft Systems (C-UAS) National Action Plan and Legislative Proposal, U.S. Department of Justice (April 25, 2022).
- Audit of the Department of Justice's Efforts to Protect Federal Bureau of Prisons Facilities Against Threats Pose by Unmanned Aircraft Systems, DOJ Inspector General, Audit Division, 20-104 (September 15, 2020). ♦