Eyes in the skies

The latest threat to correctional institution security

By Todd R. Craig, Joe Russo and Dr. John S. Shaffer

***Authors' Note:** Findings and conclusions reported in this article are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice (DOJ). The products, manufacturers and organizations discussed in this document are presented for informational purposes only and do not constitute product approval or endorsement by DOJ.*

Unmanned aerial aircraft systems (UAS), or unmanned aerial vehicles, pose a threat to correctional agencies throughout the world. This threat is not simply theoretical or merely plausible. There have been multiple incidents reported worldwide where handguns, cellphones, drugs, tobacco, pornographic DVDs, implements for escape and other contraband have been deposited on prison grounds by UAS-operating conspirators on the outside. This threat will only increase as UAS become more ubiquitous. According to UAVGlobal.com, there are 441 known UAS manufacturers worldwide.[1] Figure 1 shows the UAS sales forecast summary for the U.S. over the next five years, according to a recent Federal Aviation Administration (FAA) report.

Figure 1. U.S. UAS Sales Forecast Summary 2016–2020 (in millions)

	2016	2017	2018	2019	2020
Hobbyist (model aircraft)	1.9	2.3	2.9	3.5	4.3
Commercial (non-model aircraft)	0.6	2.5	2.6	2.6	2.7
	2.5	4.8	5.5	6.1	7.0

Reported UAS incidents

UAS incidents at prisons have been reported in the U.S., Canada, Mexico, Ireland, Australia and the United Kingdom. In the U.S., correctional authorities in Wisconsin, Colorado, Minnesota, New York, Virginia and several Federal Bureau of Prisons facilities reported UAS flyover incidents. It is unknown whether these flyover incidents involved innocent hobbyists or people with a more sinister intent. Many experts believe the actual number of corrections-specific UAS incidents is unknown and may be grossly underreported.

UAS flyover incidents create an adverse operational impact on facilities where incidents occur. These facilities have to be locked down and searched, which requires a significant amount of manpower and overtime costs to complete. In December 2015, a handgun was delivered via UAS to the Rivière-des-Prairies Detention Centre in Quebec, Canada. Mexico reported UAS drug deliveries, and in the U.S. UAS incidents involved contraband in multiple states, including California, Maryland, Georgia, Ohio, South Carolina and Oklahoma.

As depicted in Figure 2, UAS and contraband were intercepted by the Maryland Department of Public Safety and Correctional Services on Aug. 22, 2015, outside the Western Correctional Institution in Cumberland, Maryland. A Yuneec Typhoon, a UAS-type vehicle, and contraband included tobacco, synthetic marijuana, prescription narcotics and pornographic DVDs. Investigators noted this particular UAS model has sufficient lift and payload capacity to deliver all of the contraband seen in the photograph, with the exception of the handgun found in the UAS operator's car.

The Georgia Department of Corrections reported the arrest of four individuals who conspired to use UAS to smuggle tobacco and cellphones into the Calhoun State Prison in November 2013. Two pounds of tobacco were confiscated from the car of the UAS operator. The Ohio Department of Rehabilitation and Correction (ODRC) documented three separate UAS incidents. In January 2015, a UAS vehicle crashed at the Franklin Medical Center in Columbus. In May 2015, a UAS vehicle carrying six ounces of marijuana crashed inside the North Central Correctional Institution near Marion. In July 2015, a UAS carrying tobacco, marijuana and heroin deposited its payload at the Mansfield Correctional Institution and took off. This delivery of contraband inside the prison yard resulted in a disruptive incident as some inmates fought over the contraband and others created a diversion while some of the contraband was concealed.

In April 2015, officials at the South Carolina Department of Corrections reported a small UAS craft crashed in the bushes outside the Lee Correctional Institution in Bishopville. The UAS was carrying cellphones, tobacco, marijuana and synthetic marijuana.

Finally, the Oklahoma Department of Corrections (ODOC) reported an incident in October 2015 where a UAS carrying two 12-inch hacksaw blades, a cellphone, a cellphone battery, two packs of cigarettes, 5.3 ounces of marijuana and multiple street drugs crashed at the Oklahoma State Penitentiary in McAlester. A second UAS incident was reported by ODOC in March 2016, when a UAS vehicle carrying three cellphones crash-landed at the Cimarron Correctional Facility in Cushing.

Detection and mitigation solutions

UAS are sold in a variety of sizes and capabilities, ranging from small quad-copters that cost less than $100 and have payload capacities of less than a pound, to UAS able to lift payloads of 100 pounds and costing tens of thousands of dollars. The simplest UAS use direct, radio-frequency (RF) remote-control signaling to control the device, while more advanced UAS employ GPS guidance that does not require any direct user control inputs. An emerging component-parts industry, servicing both the commercial and hobbyist market, will allow individuals to modify and custom-build contraband delivery UAS. Custom-built UAS could escape acoustic detection and would be virtually untraceable if it was recovered by authorities after a crash. The set of potential threats for a correctional facility is dynamic and expanding.

Designing countermeasures to these threats is an evolving and complex task. The range of technology solutions designed to combat UAS threats can be classified into one of two approaches: detection solutions and mitigation solutions. UAS detection technologies fall into one of two types: passive and active. Passive solutions use multiple sensors that monitor the environment. Passive technologies include radio frequency detection systems, acoustic detection systems, video surveillance systems, thermal imaging/infrared (IR) devices and/or seismic (vibration) sensor systems. These solutions apply software analytics to track the location of UAS

Figure 2. UAS and Contraband Intercepted by MD DPSCS (Aug. 22, 2015)

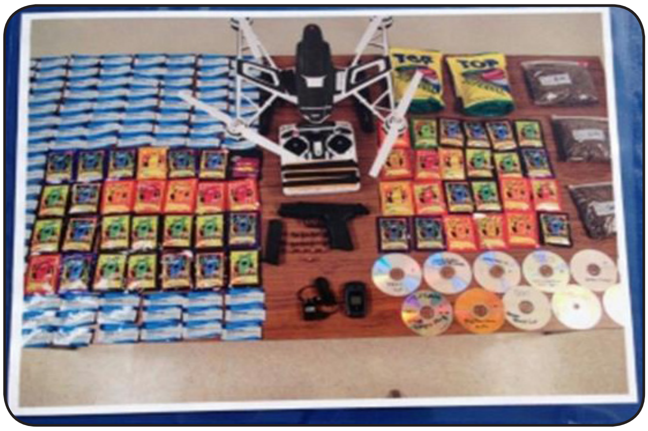


Photo courtesy MD DPSCS

Figure 3. UAS and Contraband Recovered by ODOC (Oct. 26, 2015)

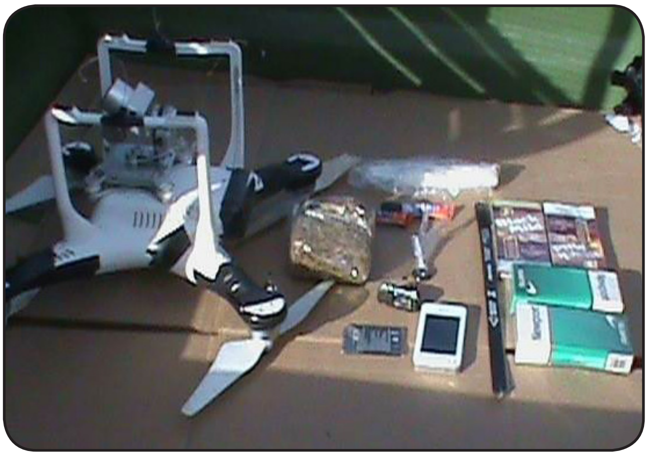


Photo courtesy ODOC

relative to the position of the deployed sensors. Active detection technologies, like radar, emit energy and detect any reflection that indicates UAS are operating in a controlled area.[2]

RF systems use an array of receivers to cover a controlled area. Effective range for an RF detection solution is limited by the characteristics of the RF signal emissions, the quality and type of receiver used, and the signal processing techniques employed. Acoustic systems use an array of sensors to detect audible emissions. When the monitored spectrum correlates to a known acoustic signature, and the direction is determined based on which sensor captured the audio signal, an alert is issued. Effective range for an acoustic system depends on the quality of the sensors, the ambient sound environment, the tuning of the sensors for the site, and the processing algorithms used. Visual detection employs night-vision capable cameras that scan the sky to detect UAS operating nearby. Visual detection solutions attempt to match the video signature of UAS to a known signature database. Directionality and location are determined by the camera(s)' "look" angle(s). Weather conditions impact system performance and effective range. Clear line-of-sight is critical to the performance of a visual detection system. The Cayman Islands and Nova Scotia have reported using UAS as aerial video surveillance platforms to enhance perimeter security at some prison sites. In response to multiple UAS attacks, ODRC evaluated a tethered "Blimp-in-a-Box" solution that provides aerial surveillance using video, IR and thermal imaging solutions. Later, they abandoned the effort, citing the poor quality of the images and the $170,000 per unit cost as factors in the decision.[3]

UAS flyover incidents create an adverse operational impact on the facilities where the incidents occur.

Thermal detection employs an array of IR cameras that scan the sky to detect UAS operating nearby. The cameras attempt to match the detected heat signature of a UAS to a known signature database. As with visual detection, directionality and location are determined by the IR camera(s)' look angle(s). Weather conditions are a key factor that impact performance and effective range. Clear line-of-sight is required. Temperature contrast of the UAS to the surrounding environment is another factor that can impact system performance. Seismic detection relies on an array of sensors implanted in the ground to monitor the vibrations induced by UAS operating nearby. They attempt to match the detected seismic spectrum signature of UAS to a known signature database. They provide highly accurate location estimates when properly tuned for the environment. The quality of the sensors, the seismic environment, the tuning of the sensors for the site and the processing algorithms are the main factors that impact performance and effective range.

Radar detection solutions actively emit electromagnetic energy and measure reflection of that energy off physical elements in the environment. UAS can be detected based on their reflected energy signature, and their flight path can be estimated. Radar systems tuned to detect small UAS also are prone to detect birds, generating nuisance alarms in certain environments. To counter that, flight-path estimation is used to differentiate avian flight from UAS. UAS are assumed to follow fairly predictable flight paths, while bird flight paths are more erratic. Also, Doppler radar captures UAS propeller movement, which is another

Figure 4. Threat Vectors

Threat Vectors

- **Aerial Surveillance — Video Monitoring of Facility Operations/Vulnerabilities/Targets**
- **Introduction of Contraband — Contraband Delivery That Circumvents Conventional Security**
- **Electronic Attack — Interception/Manipulation of Data/Communication/ Security Systems**
- **Kinetic Attack — Delivery of Weapons or Explosives to a Specific Target**
- **Weapons of Mass Destruction (WMD) Attack — Delivery of Biological/Chemical Agents**

It is likely a layered approach of low-tech policies and high-tech sensor and detection systems will provide the best overall UAS detection system for the correctional environment in the future.

characteristic that distinguishes UAS flight paths from bird activity. The main challenge with a radar-detection solution is that it operates as an emitter. As such, there are frequency-use issues that must be overcome. This aspect increases the deployment complexity of a radar system versus any of the passive detection solutions.

Some correctional agencies have adopted a low-tech approach to UAS detection. They simply advise staff that if they see or hear UAS in the vicinity of the facility, they are to report immediately. They then lock the facility down and commence a ground search for contraband. Even if technology solutions are implemented to address the UAS threat, this low-tech policy and procedure is a fundamental security response.

In addition to detection, mitigation solutions are available. Mitigating UAS threat is a much more complex task. However, there are several interesting solutions emerging. Interceptor UAS use a net to capture intruder UAS. Tests have demonstrated both the viability and the inherent complexity of this approach. A correctional facility would have to maintain its own UAS fleet, with full-time qualified operators on active-alert status, to counter intruder UAS. Operators would have only a brief window of opportunity to detect and locate intruder UAS, then make a positive identification and threat assessment before deploying interceptor UAS to take it down. To stand up, train and staff such a post 24/7 would be cost prohibitive for most correctional facilities. Even if all these measures were feasible, there are considerable legal and liability constraints that may make UAS interceptions ill-advised.

One company in the Netherlands is focused on a low-tech solution to this high-tech problem: training birds of prey to take down UAS in flight. To date, there have been no reports of using trained birds as a defense against UAS in the correctional environment. Also, a variety of "blunt-force" approaches are being explored. For example, lasers, surface-to-air missiles and basic firearms are all being evaluated as methods of taking down UAS. These solutions share one major flaw, which is the risk posed to public safety in attempting to shoot UAS out of the sky. Additionally, researchers in South Korea have demonstrated the ability to destabilize UAS in flight using sound waves. High-energy sound waves are tuned to a frequency that causes the UAS gyroscope to become unstable. Once the gyroscope is disrupted, UAS are unable to maintain flight. Again, there is concern about personal injury and/or property damage that may occur from falling UAS debris.

Some approaches seek to mitigate UAS by interfering with their communication and/or navigation capability. For example, a University of Texas at Austin research team successfully demonstrated that UAS flight paths can be redirected by "spoofing" its GPS navigational signals. Further, radio frequency jammers can disrupt the command control between the UAS and its operator. Both approaches, while technically feasible, are currently illegal per Federal Communications Commission regulations.

There is an emerging industry designed to establish "UAS No-Fly Zones" around private property sites on an opt-in basis. Property owners subscribe to a service provider who maintains an active list of voluntarily registered "UAS No-Fly Zone" coordinates. Providers have established agreements with UAS manufacturers to program their firmware to prevent them from operating over any site listed in the database. The database prohibits UAS flights over certain civil and military sites, airports and other sensitive locations.

Legal issues notwithstanding, the voluntary geo-fencing registration solution will not be effective with the existing UAS fleet or any new models not voluntarily compliant with the geo-fence code option. Future legislation may mandate UAS manufacturers comply with embedded geo-fence code requirements, but it is unlikely that the requirement could be applied retroactively to the existing UAS fleet.

Legal and policy considerations

Prior to developing UAS policies and spending money on countermeasures, a comprehensive risk assessment is required. Correctional staff should weigh the probability of UAS attack against the possible damage that it might inflict. The inherent strengths and vulnerabilities of each solution must be considered, along with the potential for adverse outcomes if the technology fails. There are also legal and policy issues that must be considered when developing a UAS defense plan. Further, agencies should periodically evaluate policy or regulatory changes that may be needed as a result of innovations or developments in UAS technology.

The FAA likely will consider the monitoring of a correctional facility by UAS to be a "commercial operation." If so, qualified FAA-licensed pilots must operate UAS. Pilots will require initial and recurrent training and appropriate relief schedules. These potential requirements add to the operational costs and liability for insurers and agencies. A correctional agency considering any UAS detection/mitigation solution would be well-advised to confer with qualified legal counsel.

Insurance and liability issues will arise with the proliferation of the UAS market. As UAS crash and cause personal injury or damages, there will be lawsuits and settlements. There are implications for several areas of the law, including personal injury, property damage, trespassing, privacy intrusion and nuisance cases. It is likely insurance products will emerge to address the liability exposure to the UAS owner based on third-party use, electronic malfunction or intentional hijacking.

As was the case when the introduction of cellphones into prisons first became an issue for correctional administrators, the exponential increase in UAS has created legal issues that are not adequately addressed by laws written before UAS were invented. It is not the first time technology has outpaced the law, and it is not the first time people with criminal intent have exploited that gap.

Multiple states have enacted legislation specifically designed to combat the adversarial UAS threat to public safety. Although FAA regulations don't expressly prohibit UAS from flying over correctional facilities, a few states are attempting to address this specific threat through legislation. To date, only Tennessee has enacted legislation that specifically prohibits "unmanned aircraft over the grounds of a correctional facility."[4] Legislation recently failed in Colorado, in part because lawmakers questioned the need for special legislation, considering that UAS being used to transport/deliver contraband to a prison is, by definition, contraband itself, an act that is already prohibited by Colorado law.

Conclusion

Although UAS-related events today are low-incidence, the threat is potentially high-impact. Much like the issue of contraband cellphones, a relatively minor problem 10-15 years ago, this threat could expand very quickly considering the rapidly growing number of recreational and commercial UAS filling the skies. Current correctional countermeasures are practically non-existent, likely to be ineffective and/or cost-prohibitive. Interceptors may not be viable; jammers are illegal; and sensors are expensive and susceptible to false alarms, and they do not provide adequate response time.

There are several emergent UAS defense technologies for correctional facilities. Each technology has strengths and limitations. Some of these technologies are already under evaluation, while others will be evaluated as they become available. It is likely a layered approach of low-tech policies and high-tech sensor and detection systems will provide the best overall UAS detection system for the correctional environment in the future. As UAS activities increase, agencies need to share information and gain awareness of and continuously reassess the threat. For now, vigilant officers and low-tech practices are probably the best response.

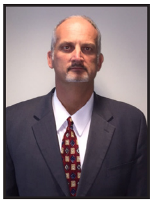
ENDNOTES

[1] *List all manufacturers*. (UAVGlobal). Retrieved from www.uavglobal.com/list-of-manufacturers

[2] Gettinger, D. (2015, March 20). *Domestic drone threats*. (Need to Know - Center for the Study of the Drone at Bard College). Retrieved from http://dronecenter.bard.edu/what-you-need-to-know-about-domestic-drone-threats

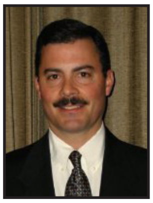
[3] Associated Press. (2015, March 23). State puts hold on drone security testing at Ohio prisons. *Akron Beacon Journal*. Retrieved from www.ohio.com/news/break-news/state-puts-hold-on-drone-security-testing-at-ohio-prisons-1.577326

[4] Associated Press. (2016, February 15). Drones pose new smuggling challenges for prison. *The Boston Globe*. Retrieved from www.bostonglobe.com/2016/02/15/drones-pose-new-contraband-smuggling-challenge-for-prisons/gqHaHGXUaiUL0WMunxBg0O/story.html



Todd R. Craig is chief of the Office of Security Technology at the Federal Bureau of Prisons.

Joe Russo is corrections technology lead at the Justice Technology Information Center/ National Law Enforcement and Corrections Technology Center System.



John S. Shaffer, Ph.D., is institutional corrections subject-matter expert at the Justice Technology Information Center/National Law Enforcement and Corrections Technology Center System.