TECH b•e•a•t

Dedicated to Reporting Developments in Technology for Law Enforcement, Corrections, and Forensic Sciences

No More 'Cell' Phones

In the late-night quiet of a prison cellblock, an inmate slips his hand into a small slit under his mattress and pulls out a cell phone. Speed dial connects him to his outside contact, he speaks a few prearranged words, and another drug deal is made. Technology—albeit contraband technology—allows him to operate as if he were still on the streets.

As cell phones become smaller, it becomes easier to smuggle them inside correctional facilities. It becomes easier for inmates to continue their criminal activities, harass victims, or transmit photographs of supposedly secure information.

Fortunately, in today's technology-driven society, when one innovation creates a problem, a new innovation usually comes along to solve it. But for correctional officers and administrators, the question becomes where to find the right innovation.

"The scope of the problem is this: we are trying to get cell phones out of prisons or at least render them useless," says Ike Eichenlaub, chief of the Federal Bureau of Prisons' (BOP's) Office of Security Technology. To date, several possible technology approaches have been identified to deal with the cell phone problem in prisons and correctional facilities:

Locate cell phones and confiscate them. This approach, Eichenlaub says, requires a technology that, at a minimum, will—

- Work even when cell phones are turned on for only a few minutes at a time.

- Detect signals emanating from any area of a facility.

- Find transmissions through thick concrete walls, in buildings that range from single story to multifloored, and in locations varying from urban downtown areas to remote rural districts.

Ideally, he says, such a technology would require minimal or no training to use; expand to cover other wireless technologies, such as two-way pagers; and operate on a 24/7 basis.

Overpower the signal with a stronger signal. "Another potential approach is commonly referred to as 'jamming,' which emits a signal stronger than a cell phone's signal and renders it useless," Eichenlaub says. Senior BOP Technologist Jim Mahan adds, "There are two types. One is called brute force jamming, which just blocks everything. The problem is, it's like power-washing the airwaves and it bleeds over into the public broadcast area. The other puts out a small amount of interference, and you could potentially confine it within a single cell block. You could use lots of little pockets of small jamming to keep a facility under control."

"Trick" the phone. Eichenlaub describes a third possible approach, commonly called "spoofing," as tricking the cell phone into thinking a "no service" signal is coming from the nearest cell tower.

The Federal Communications Commission, however, prohibits both jamming and spoofing, he says, so implementing either of these technologies would require legal and regulatory changes.

Intercept the signal. A fourth possible approach, signal interception, retrieves the telephone and serial numbers from operational phones, but it can be implemented only under a judge's order.

Eichenlaub says that although signal interception is feasible, "We are looking for the simplest option, which is signal detection. There are no regulatory or legal issues here; if you can find it, you can go get it."

Different cellular providers use different communications protocols, but all cell phones use radio frequency (RF) antenna power. BOP has studied a number of off-the-shelf technologies to detect RF signals. Although a variety of detection equipment is available, costs can reach tens of thousands of dollars. "Some [technologies] work better than others," Mahan adds. "Some work for only a short distance, maybe about 15 to 20 feet. This is impractical if you're trying to cover 50 acres. Also, each device may cost about $1,000. There is some promising new

technology that is showing better results than anything else we've ever seen, but they are still prototypes. The question is whether the technology can be made at a cost that we can afford. Vendors would need to reengineer solutions originally developed for other professions, such as the military, first responders, or law enforcement."

"I think that a solution can be developed, but there are none out there that meet BOP's needs right now," Eichenlaub adds.

In response, BOP, the National Institute of Justice (NIJ), and the Naval Surface Warfare Center–Dahlgren are collaborating on a multiyear project to evaluate the problem and ultimately help that technology develop. BOP spent the first 6 months of 2004 evaluating and testing various possibilities. Now Dahlgren staff members (with NIJ funding) are going to evaluate the entirety of the problem and potential technical solutions to provide a roadmap to addressing this problem. In the course of this evaluation, they will—

- Analyze and document BOP's work.

- Discuss this issue with the American Correctional Association and the Association of State Correctional Administrators to ascertain the needs of State and local correctional institutions and determine how they might differ from BOP requirements.

- Assess the spectrum of potential approaches and technology solutions.

- Ultimately, incorporate BOP's work and other information into a report that recommends NIJ's next technology development steps.

Chris Tillery, project manager for NIJ, says he expects that report to be completed and released later in FY 2005

For more information on the Federal Bureau of Prisons' research into cell phone use by inmates, contact Ike Eichenlaub, 202–305–8448 or LEichenlaub @bop.gov. For more information on the National Institute of Justice's involvement, contact Chris Tillery, 202–305–9829 or george.tillery@usdoj.gov.