

## **The Darker Side of Mobile**

Someday, everything will be 'always connected' with any one or multiple of cheap and readily wireless technologies. With growth industries in GPS navigation, sensor networking, social networking and Google Maps the virtual and physical worlds are on a collision course that is unstoppable. Maybe not tomorrow, but in the not-to-distant future the always-connected world we live in will affect every correctional facility in the world from both a wireless and wired perspective. It is important for decision makers to know what the solutions are and how to implement them.

The convergence of the physical and logical worlds, along with the impact of wireless technologies is most easily observed as being huge threats in security-centric markets such as Corrections. Two things must happen to ensure the protection of lives and property, as well as maintain enforcement of laws and policies that govern these environments. First, physical and logical security surveillance systems must be thought of holistically and no longer distinct or separate. Second, innovative and adaptive wireless surveillance systems capable of supporting future radio protocols must be employed to ensure that the next great thing available today to billions of consumers around the globe don't become the new and easy method of circumventing the systems in place at these highly protected and sensitive facilities.

In this article, the focus will be the challenges that the convergence of physical and logical security present to correctional practitioners and those responsible for the safety and security of inmates and staff and proprietary information on them. In addition, the article will discuss a number of 'best practices' and next steps and possible solutions that will keep correctional facilities in adherence with the strictest security protocols possible.

In a correctional environment, when everything is always connected, it means a number of things along two dimensions. In the first dimension, it will mean improved security. Management and line staff will be able to count, track, and communicate with all mission critical assets. This includes inmates, staff, keys, weapons, radios, cameras, sensors, alarms, personal computers, etc. When everything is Always Connected the network will become a force multiplier that will allow more automation and fewer staff doing the work that used to be done by a much larger staff focused on maintaining the facilities physical security.

However there is a darker side to the mobile and wireless technologies that enable this always-connected experience. In the hands of inmates many of these current and future technologies embodied in vast quantities of readily and commercially available consumer electronics will have the potential to seriously compromise the security of both the physical and IT network infrastructure of a correctional facility. As a recent video and article from the California Department of Corrections and Rehabilitation website on contraband cell phones in prisons points out, the

consumer electronics industry is spending billions of dollars making their equipment smaller, smarter, more sophisticated and loaded with high tech features. While this is going on, the correctional industry is spending pennies trying to counter the flow of consumer electronics smuggled into correctional facilities.

Inmates with cell phones in prison are just the first symptom of a more serious problem that will continue to mutate until correctional management is forced to spend significant resources to protect their physical and IT security infrastructures in order to retrieve the technologies from the inmates. A major part of this expenditure will need to be in systems that bridge the physical and logical security infrastructures, once being very distinct but now headed on a collision course to converge. Closed-circuit video surveillance systems over twisted pair analog circuits are migrating to IP video cameras connected over IP/Ethernet networks.

Those networks can be wired Category-5 cabling or wireless backhaul technologies such as WiFi bridging or wireless mesh networking. Perimeter fencing to keep intruders out and inmates in are being augmented with wireless sensor networks for “geofencing”, locating, and tracking cell devices, WiFi devices, RFID tags on mechanical or human assets, and GPS devices for the tracking of all individuals within a secure perimeter in order to improve life and safety issues for all. These logical sensing systems will increasingly monitor daily environmental, human presence, and overall safety conditions in a corrections facility. The central access monitoring and control stations will be augmented by this physical and logical security convergence in order to maintain the usability from the perspectives of the non-technically oriented corrections officers.

Correctional management may not yet realize that physical and logical security systems have already started to converge. Inmate management software, inmate pictures, radios, CCTV-to-IP video, and perimeter fence sensors are just a few of the first steps into the future integrated digital security network where everything will be always connected. Yet so much more needs to be done. One particular change required is to accelerate the adoption and procurement processes of these integrated wireless and digital technologies. Many times the systems that are installed into a corrections facility end up having been obsolete by months or years due to the slow process of government procurement. Physical security systems traditionally did not change or innovate as rapidly as IT systems, but that is changing as well. In all levels of government agencies and services we are seeing changes in practices of accelerating the evaluation, adoption, and procurement of these commercial off-the-shelf technologies to facilitate the physical-logical convergence. In order for these processes to accelerate, a closer partnership between the public agencies and organizations managing the correctional facilities and systems, and the private sector companies that are on the leading edge of innovation in this unstoppable trend towards physical-logical security convergence.

There is incredible innovation and widespread adoption of cellular technologies some of which fit into a wristwatch. Smartphones that fit in a pocket have

capabilities that put personal computers of the 1990s or mainframes of the 1980s to shame. Sensors as small as a fingernail or grain of rice are capable of monitoring humidity, movement of a door or fence, or presence of explosive devices. Increased commoditization of mobile voice and data technologies enable these “connected” devices to be smaller, smarter, cheaper, possess longer battery life, and be easily obtainable through a myriad of purchasing methods.

Consumer electronics manufacturers move huge volumes of these devices through online channels, retailers, and other more specialized outlets. Increasingly these consumer electronics devices, whether it is a game pad, digital picture frame, smartphone, laptop, or netbook will contain a wireless connectivity technology (sometimes two or more) for accessing Internet information or enable connectivity for voice or messaging among groups of people. While connectivity to these mobile Internet networks is not free, there are zero barriers to obtaining a prepaid account that includes voice minutes, buckets of text messages, and possibly mobile data connectivity for \$20 or \$30. The mobile networks operators and their device and equipment manufacturers spend millions of dollars in marketing and sales incentives every year to drive the rate of adoption, geographic penetration, and their own marketshare to achieve one thing up and to the right—average revenue per user. This is the lifeblood of the mobile network operators and every participant in their respective ecosystems in terms of their profitability. There is nothing wrong with competing and making a profit in a capitalistic society. However, the same innovation and financial best practices can go into creating technologies and systems for more altruistic purposes such as preventing loss of life, enforcement of general public safety, and bettering conditions for those corrections officers that put their lives on the line every day.

A combination of innovations that have occurred in longer battery life, advanced power management, and embedded applications and operating systems can be applied in a corrections context to building adaptive, frequency agile wireless systems used for data transport (IP video surveillance), asset tracking (keys, weapons, people), and sensing for security threat detection and management (contraband cell phones, unauthorized consumer electronics devices, perimeter “geofencing” and monitoring of entry/exit throughout corrections facilities). The same 700MHz spectrum that will hopefully one day be put to use for novel mobile broadband applications can be applied in a corrections facility for robust wireless communications systems given the ideal propagation characteristics of that particular spectrum. Frequency agile wireless protocols being developed for the new UHF TV band spectrum vacated in June 2009 can also be used to build frequency agile wireless backbone systems in corrections institutions transporting the sensor systems, IP video surveillance, and other critical converged applications while exhibiting a robustness and resilience to any threats posed by inmates or outside sources to disruption or interference. It is a well-known fact of the inmate “underground” network that when a hole in the security system is identified, the news travels fast throughout the country to other correctional institutions and inmate populations. Perhaps one of the first and oldest social networks in human

civilization started with the “brotherhood” of prisoners and wrongdoers. Today with the Internet, there are even more opportunities to network and socially connect billions of people all around the planet. So with these same tools for the mass market, the inmates will find ways of leveraging them as well.

## **Considerations**

Thornton Wilder once said, “I know that every good and excellent thing in the world stands moment by moment on the razor-edge of danger and must be fought for.” The emergence of the Internet has ushered in an era where there are no longer barriers to sharing information, connecting and communicating with anyone else in real-time, and enhancing the increasingly blurred personal and professional lives people lead today. The trend towards the convergence of physical and logical security systems enables much more operational efficiency, cost effectiveness, and removal of duplicate or fragmented system silos. Mobile technologies and devices, especially when coupled with both the Internet and physical-logical security convergence untethers the corrections officers and support staff from a console screen, a desk phone, a personal computer, or generally a fixed area where they cannot maximize their productivity and situational awareness of the activities and environment around them. But there is also the darker side to these technological marvels of mankind.

As inmates become more equipped with contraband electronics, their ability to electronically vandalize or disable mission critical infrastructures will grow exponentially. Because of the electronics, software, and communication protocols found in modern physical security equipment, correctional management must insist that their new equipment is equipped with necessary digital/IP security measures to ensure that it can withstand the internal and external threats that might be used against it. Additionally, correctional staffs that manage these systems must be trained in inmate management and digital/IP security. Correctional IT staff must be able to fully recognize that there is another component to their jobs which includes physical security of correctional facilities using the resources that used to be totally dedicated to computer networks. Correctional IT staff and correctional custody staff must also recognize that equipment on a shared correctional LAN (local area network) can be a personal computer or a security device such as a IP camera. They are both just one type of many terminals that must be on a network in order to be cost effective and maximize the utility of the wired and wireless networks.

In the future, vast internal networks of sophisticated sensors will facilitate the micro-management of inmates as they move throughout a correctional facility. These sensors will allow management to detect individuals, their movement and direction, equipment, locations, weight, fire, smoke, and a vast array of other things, allowing for total accountability of everything within or around a secure correctional facility. The Warden will truly know all and be able to see everything within his or her facility.

Co-Authors:

Jim Mahan  
Senior Technologist, Office of Security Technology  
US DoJ Fed Bureau of Prisons  
(202) 307-3191, x3  
320 First St. NW  
Washington, DC 20534  
[JMahan@bop.gov](mailto:JMahan@bop.gov)

Ozzie Diaz  
President & CEO  
AirPatrol Corp.  
(866) 430-4227, x231  
9861 Brokenland Parkway, Suite 204  
Columbia, MD 21046  
[odiaz@airpatrolcorp.com](mailto:odiaz@airpatrolcorp.com)