Analysis of Managed Access Technology in an Urban Deployment: Baltimore City Jail Complex

Fred Frantz
Engility Corporation

Phil Harris
Engility Corporation

Engility Corporation, Rome NY
Award Number: 2010-IJ-CX-K023

September 2015

Table of Contents

List of Tables

List of Figures

Acknowledgement

The authors would like to thank Nancy Merritt, Joseph Heaps, Jay Miller, Secretary Steven T. Moyer and Casey Joseph for their support of this project, as well as their insights throughout its completion.

Executive Summary

Managed access, as a category of technology, has become an increasingly significant tool for denying illegal inmate use of cellular telephone services. This report is the second of a set of reports examining the impact of managed access technology on contraband cell phone use in prisons. The focus of this report is the use of Distributed Antenna System (DAS) Technology, deployed in support of cellular Managed Access System (MAS) use in an urban correctional facility—the Maryland Department of Public Safety and Correctional Services (DSPCS) Baltimore City Complex. This report builds upon technical information in a previous assessment of MAS which described operation of managed access technology deployed in a rural correctional facility. The technical background material is presented in a conceptual format rather than providing detailed implementation specifics.

This study concludes the following:

1. While managed access had a significant impact within the facilities where it was deployed, other factors unrelated to the technology such as policy changes also contributed to the overall decline of illegal cellphone use throughout the prison system (to include faculties with deployed managed access systems).
2. Good working relationships with nearby cellular carriers are critical.
3. MAS can effectively be implemented in an urban setting. Technology such as Distributed Antenna Systems (DAS) allows operators to refine and control system coverage within tightly constrained environments.
4. DAS deployment is heavily reliant upon physical installation of cable, conduits and other supporting infrastructure. Retrofitting an existing correctional structure is particularly challenging with unique logistical challenges involved with deploying it in areas where inmates reside and securing the system infrastructure from sabotage.
5. Cellular managed access technology only addresses cellular communications capabilities and cannot, for instance, prevent use of non-cellular wireless capabilities, such as Wi-Fi, stand-alone computing or photographic capabilities which have become standard features in modern cellular devices. Managed access mitigates the connection of cellular radio transmissions between a handset and an external (e.g., commercial) network. Elimination of cellular communications capabilities makes other features present in these devices less useful to the inmates that possess them.

Introduction

This report is the second of a set of reports examining the impact of managed access technology on contraband cell phone use in prisons. The focus of this report is the use of Distributed Antenna System (DAS) Technology, deployed in support of cellular Managed Access System (MAS) use in an urban correctional facility—the Maryland Department of Public Safety and Correctional Services (DSPCS) Baltimore City Complex. This report builds upon technical information in a previous assessment of MAS which described operation of managed access technology deployed in a rural correctional facility (the Mississippi State Penitentiary in Parchman, MS)[1], referenced as the "Parchman Report" in the remainder of this report. As with the Parchman Report, much of the technical background material presented herein is presented in a conceptual format rather than providing detailed implementation specifics.

Managed access technology has become an increasingly significant tool for denying inmate use of cellular telephone services. Managed access, in contrast to radio frequency jamming, or passive signal sensing, selectively denies service to unauthorized users.[2] Passive radio sensing is another category of technology described in the Parchman Report. Passive sensing provides an alternative approach to interdiction of illegal cell phone use, one which recognizes cellular radio signals and alerts a system operator of an active wireless device. Stated in another way, passive sensing technology works in a "listen only" mode which informs physical intervention by prison

[1]Grommon, E., Carter, J., Frantz, F., Harris, P., *A Case Study of Mississippi State Penitentiary's Managed Access Technology*, report to the National Institute of Justice, August 2015, currently under publication review.

[2] Jamming technology is currently illegal for non-Federal users. The Communications Act of 1934, Section 333 - prohibits willful or malicious interference with the radio communications of any station licensed or authorized under the Act or operated by the U.S. Government (47 U.S.C. § 333). It is a violation of federal law to use a cell jammer or similar devices that intentionally block, jam, or interfere with authorized radio communications such as cell phones, police radar, GPS, and Wi-Fi, see http://www.fcc.gov/encyclopedia/jamming-cell-phones-and-gps-equipment-against-law

staff. Unlike managed access or jamming technologies, passive technology cannot directly intervene or mitigate access to cellular services.

In contrast to passive technologies, managed access technology is an active (licensed) technology. Managed access technology is designed to actively manage service requests from cellular devices providing the ability to selectively allow or deny cellular communications to/from cellular devices. Service in this context is limited to voice and/or data calls from cellular devices on cellular network frequencies. Unlike jamming technology, managed access technology mitigates communications to/from approved cellular devices so that legitimate calls be processed and completed, while cellular network service requests to/from non-approved, presumably contraband cell phones are legally disrupted. Managed access use is guided by operational policy and guidelines of the deploying agency[3].

Managed access technology "manages" cellular network services available to specific cellular users and/or cellular devices. Like cellular jamming technology, managed access systems actively transmit radio signals on cellular network radio frequency bands so they are subject to FCC licensing, or NTIA authorization[4,5]. From an operational perspective managed access capabilities and operational effectiveness are relatively new topics and subject to agency choices related to system architecture, system deployment details, and ongoing operation. Total cost of ownership, system functionality, and actual impact on cell phone use, both within and

[3] This report uses the terms "call" and "connection" in this document interchangeably to describe a request for service (voice, messaging via text/email/multimedia and/or Internet access) placed from a cell phone via a commercial cellular network.

[4] This includes bands associated with the commercial cellular service, broadband personal communications and certain advanced wireless services.

[5] In this paper the terms "active" and "passive" used in context of regulatory and licensing describe technology that actively transmits radio energy using frequencies within commercial mobile service bands (active) or only receive signals in these bands (passive). This is in contrast to usage that describes operational capability, i.e., technology that "passively" disables the use of cellular services from a distance, in contrast to those that simply provide the ability to locate an illegal device; requiring "active" intervention on behalf of prison personnel to seize and disable the illegal devices. Both uses appear in this paper.

outside of the designated managed access coverage area, are topics that can benefit from increased knowledge. Each managed access system deployment will have unique design and implementation challenges associated with both the physical implementation and the local commercial cellular environment within which it resides. This report seeks to further inform the decision process, complementing the Parchman Report by describing an active system operating in an urban environment; specifically managed access systems deployed in the Baltimore MD City Jail Complex.

This report is not a product evaluation; the purpose of this report is to document the managed access use in Baltimore MD, specifically:

- To examine MAS technology operating at correctional facility in an urban setting;
- To describe the use of Distributed Antenna System technology (DAS); and
- To describe how managed access technology using DAS contrasts with managed access using macro-cellular technology[6].

The Baltimore City Jail Complex

The Baltimore City Jail Complex is operated by the DPSCS and consists of the Baltimore City Correctional Center (BCCC), the Metropolitan Transition Center (MTC), The Baltimore City Detection Center (BCDC), the Chesapeake Detention Facility (CDF) and the Baltimore Central Booking and Intake Center (BCBIC). Only the MTC and BCDC have managed access systems.

[6] Use of the term "macro cell site" in this report describes use of a small number of relatively high-power base stations located in cell sites designed to cover a large area (for example in a correctional facility located in a rural setting.) This is in contract to small cell and DAS technologies described n this report.

Source: Google Earth.
Annotations: Phil Harris Engility Corporation

Figure 1. The Baltimore City Jail Complex

The Metropolitan Transition Center (MTC)

The Metropolitan Transition Center in Baltimore was built in 1811 and it is the nation's oldest correctional facility. It houses 698 offenders in a minimum security setting. The MTC is operated by the DPSCS and inmates at this facility serve time as the result of a court imposed

sentence. The FY2015 DPSCS appropriation for MTC was $41,402,746 with 393.6 authorized positions. [7]

The Division of Corrections Annual Report Fiscal Year 2013 states that the MTC offers high school equivalency diplomas (GED) in reading, writing and arithmetic and provides intensive substance abuse treatment through Therapeutic Communities, a program that treats about 200 offenders a year.[8] Training programs offered by the Maryland Department of Labor, Licensing and Regulation, through the Occupational Skill Training Center include state certification programs in automotive repair and maintenance, roofing, HVAC, information technology, warehousing, carpentry, printing and graphics and plumbing. MTC inmates do not participate in outside details.

The Baltimore City Detention Center (BCDC)

The Baltimore City Detention Center was originally constructed as a jail in 1806. It has been renovated 11 times between 1859 and 1999[9]. In 1991, Baltimore City Jail consisted of seven buildings: five of these were maximum- and medium-security structures. Minimum-security inmates were housed in two satellite facilities. In July 1991, the State took over administration of the jail from the city, and renamed it the Baltimore City Detention Center under the Division of Pretrial Detention and Services (Chapter 59, Acts of 1991)[10]. The BCDC now primarily consists of four buildings: the Women's Detention Center (WDC), the Men's Detention Center (MDC), the Jail Industries Building, and the Wyatt Building. The current WDC was opened in 1967 to house female detainees. The FY2015 DPSCS appropriation for BCDC was $85,338,930 with

[7] http://msa.maryland.gov/msa/mdmanual/22dpscs/html/dpscs.html#baltimore
[8] http://www.dpscs.state.md.us/publicinfo/publications/pdfs/DOC2013AnnualRpt.pdf
[9] http://www.mgaleg.maryland.gov/Pubs/Committee/2013-legislative-policy-committee-june.pdf
[10] http://msa.maryland.gov/msa/mdmanual/22dpscs/html/22agen.html

748 authorized positions[11]. Following corruption issues publicized in April 2013, $22.7 million has been provided to improve security and staffing within BCDC. Approximately $15.6 million has been provided to upgrade security cameras, implement a cellular managed access system, install x-ray machines, metal detectors and purchase intelligence software[12].

The BCDC is one of the largest municipal jails in the nation; over 40,000 inmates are committed to the center annually. The daily number of inmates averages over 2,000 of which about 100 are post-sentencing; the remainder are very transient (though there are also a significant number of people who have been released and are returned). Even though the BCDC is a city facility it is operated by the state. It is a jail; inmates typically are serving sentences of less than 18 months. The BCDC is also a pretrial detention facility for any person committed or transferred to the custody of the Commissioner of Pretrial Detention and Services. The Center may house any person held in custody by any agency of the Department of Public Safety and Correctional Services. In January 2015, a bill was introduced into the state legislature to transfer ownership of BCDC from the state back to the City of Baltimore.[13]

Nearby Jail Complex Facilities

There are additional facilities operated by the Division of Corrections located nearby, including: [14]

- The Baltimore Pre-Release Unit (BPRU) and Occupational Skills Training Center (OSTC).

[11] http://msa.maryland.gov/msa/mdmanual/22dpscs/html/dpscs.html#baltimore
[12] See http://mgaleg.maryland.gov/2015RS/fnotes/bil_0000/hb0210.pdf
[13] Maryland House Bill 210 has been introduced in 2015. It will abolish the Division of Pretrial Detention and Services within the Department of Public Safety and Correctional Services; providing for the transfer of property, assets, licenses, credits, and rights of the Baltimore City Detention Center to the Mayor of Baltimore City; requiring the State to pay all the operating and capital costs of the Baltimore City Detention Center in fiscal years 2016 through 2018 and one-half the costs in 2019; providing that Baltimore City pay all the operating and capital costs in fiscal year 2020. See http://mgaleg.maryland.gov/webmga/frmMain.aspx?id=hb0210&stab=01&pid=billpage&tab=subject3&ys=2015rs
[14] http://www.baltimoresun.com/news/maryland/bs-md-youth-jail-20150513-story.html

- The Chesapeake Detention Facility (CDF).
- The Maryland Reception Diagnostic and Classification Center (MRDCC).
- The Baltimore City Correctional Center (BCCC).
- The Baltimore Central Booking and Intake Center (BCBIC).

Technology and Illegal Cell Phone Management

The illegal use of contraband cell phones by inmates to access commercial cellular services continues to present operational challenges to correctional agencies and jail operators. The term "cell-phone use" in this report, specifically in the context of managed access, is the use of an illegal cellular device in a prison or jail to obtain commercial cellular voice or data services. The term "managed access" describes a category of technology or process, rather than a specific commercial product. Managed access systems from multiple vendors are currently in service, or authorized for deployment, in California, South Carolina, Texas, Maryland and Mississippi (see FCC NPRM 13-58 page 6, 2013). In early 2015 the Alabama Department of Corrections requested funds to install managed access technology at four correctional institutions [15]. Fundamentally, all managed access products are deployed to accomplish the same task: to disrupt illegal cellular communications. Managed access technology is being deployed or considered for deployment because, unlike jamming technology, FCC regulations facilitate a legal path for its adoption and use. The use of jamming technologies has been publicly demonstrated and the effectiveness of jamming technology in some venues has also been documented.[16] This report acknowledges jamming technology as a potential alternative for which legality is currently under debate. This report neither advocates for jamming, nor suggests that

[15] See http://www.al.com/news/index.ssf/2015/04/alabama_prisons_planning_syste.html#incart_river
[16] For more information about jamming see http://www.wjbf.com/story/21716332/sc-prison-cell-phone-jamming-demonstration-conducted
and http://www.ntia.doc.gov/files/ntia/publications/contrabandcellphonereport_december2010.pdf
and http://wisconsinlawreview.org/wp-content/files/3-Fitzgerald.pdf

jamming is unsuitable for mitigation of illegal cell phone use. As of the writing of this report, radio frequency jammer use by non-Federal agencies remains illegal in the United States and evaluating it as a technology is beyond the scope of this report.

As this report was written many regulatory aspects specific to MAS deployment and implementation continue to be under FCC regulatory review. FCC proceedings are underway to examine deployment regulations to include cellular network spectrum lease issues and carrier notification obligations to MAS operators following changes in nearby commercial cellular networks. The impact of these proceedings on future managed access deployment and operation will remain unknown until the proceedings are complete.

Generic managed access functionality was documented in the Parchman Report, and is re-published as Appendix B: Managed Access Technology, of this report to provide complete context for the following discussion. Readers unfamiliar with the concepts of managed access technology should read the Appendix before proceeding through the remainder of this report. This report emphasizes managed access using distributed antenna systems (DAS) based radio access network technology. The Parchman Report described a different approach, the use of more traditional macro site technology, as deployed at a rural correctional facility. Technologies like DAS (and small cells) were not addressed in the Parchman Report because they were not part of that system.

Details of cellular provider networks near these correctional facilities and/or related cellular technology protocols are not provided. Since this report is not a product evaluation, specific managed access system network interfaces and vendor-specific product features are not described. Terminology used is intended to be generic with exception to references specific to

the system provider for the agencies noted in this report[17.] Each deployment of managed access capability will have the similar goals, but to achieve those goals each system needs to be designed to address location-specific unique physical and environmental characteristics regardless of the chosen managed access technology, or product. Each system design is dependent upon facility-specific physical constraints and characteristics of the local commercial wireless environment. Because of these unique requirements, concepts associated with the topic of managed access coverage are presented in a generic manner, independent of venue-specific implementation choices.

Network Coverage and Managed Access

Wireless coverage associated with a managed access system radio access network (RAN), and how the RAN interacts with nearby commercial cellular networks, is a baseline consideration for any managed access deployment, regardless of the underlying technology used to establish this coverage. Managed access technology is used to establish a RAN that is in essence a multi-carrier multi-band cellular network, of limited scope and coverage. Managed access system RAN coverage is designed to present the dominant network signal within its designed coverage area; an area legally defined by geographical boundaries established in FCC approved cellular carrier spectrum leases. RAN coverage may be designed to span an entire correctional facility or at a minimum, coverage within specific areas within that lease area deemed by correctional officials to present the greatest risk. The managed access RAN presents itself as an extension of nearby commercial cellular networks, allowing it to capture transmissions from cellular user devices (e.g., cell phones, cellular equipped computers/tablets).

[17] Being generic also avoids the pitfalls of using endless variation of technical jargon associated with multiple generations, and versions, of cellular networking technology currently in use; each of which must be addressed by cellular mitigation technologies.

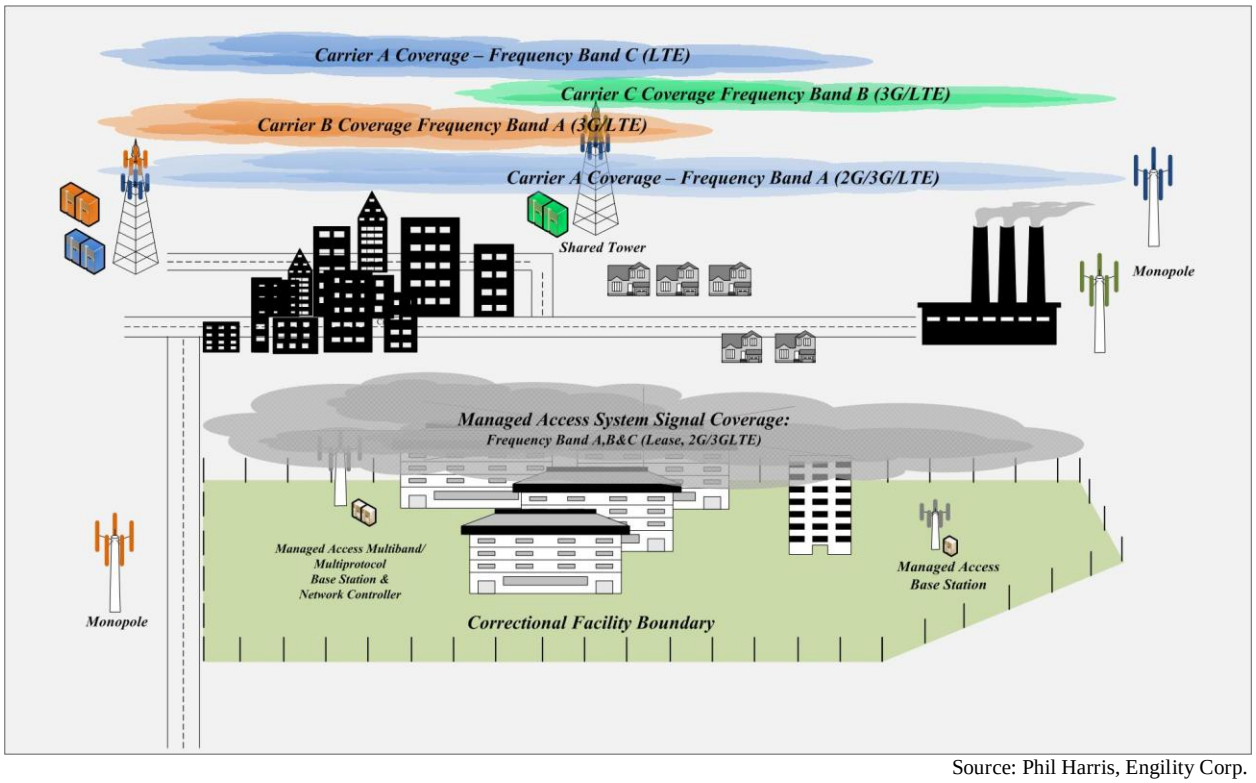
Managed access processes control all cellular communications capabilities associated with devices connected to the RAN.

The topic of RAN coverage is presented, in a simplified way, in Figure 2 and **Error! Reference source not found.**[18.] Areas with grey shading are intended to depict managed access RAN coverage as an underlay to commercial network RAN coverage. Note that a managed access system operator has a legal obligation to ensure that system coverage is contained within areas/parameters defined by their spectrum lease. This is in contrast to an operational need to establish and verify managed access operational effectiveness inside of its defined coverage area. A managed access RAN is activated and calibrated so that meets obligations associated with carrier spectrum leases and FCC rules first followed by optimizations related to effectiveness. Ongoing compliance testing requirements and methodology related to spectrum lease. Compliance testing can occur on a regular schedule or in an ad-hoc fashion; exact requirements and testing procedures need to be defined via spectrum lease details.

After all spectrum-lease lease obligations are achieved and confirmed through testing, the system can be further optimized to minimize coverage holes and maximize operational effectiveness inside operational boundaries. Testing obligations and methodology associated with ongoing managed access performance goals, related to operational effectiveness within coverage boundaries, are completely agency-defined because agency operational goals are not constrained by mandatory spectrum lease or Federal regulatory constraints. Operational requirements within the coverage area should be documented in a concise technical manner by the deploying agency, and clearly defined as a performance requirement in procurement documents if the deploying agency intends to make ongoing performance verification part of a

[18] RAN coverage depicted in this way is acknowledged to be overly simplistic from a technical perspective, but adequate to convey concepts.

contractual requirement. Costs associated with operational performance testing obligations must be understood by system operators, system suppliers, and end users. If an agency intends to use internal agency resources for recurring performance testing, then the associated operational costs and testing methodology should be well defined.

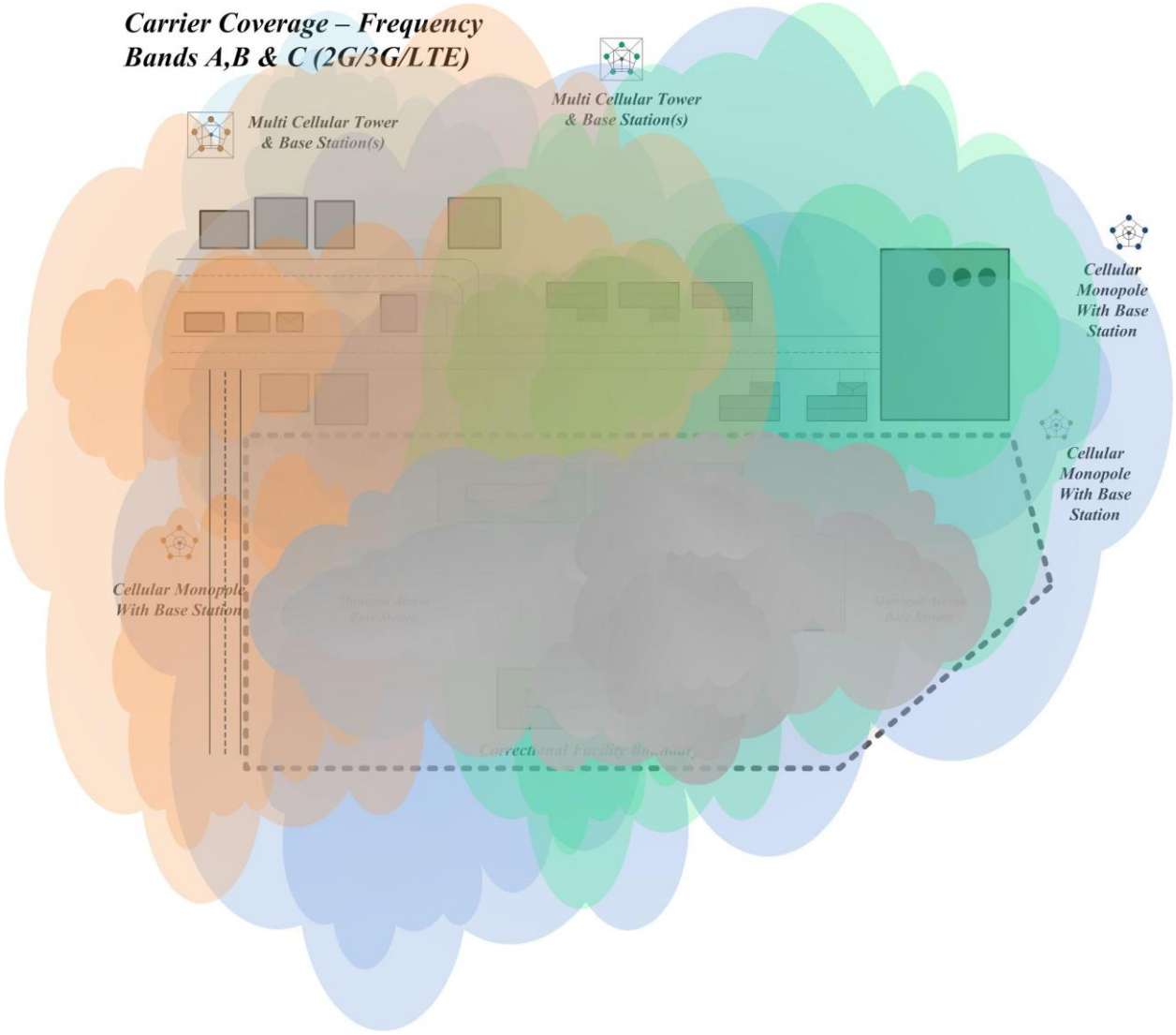


Source: Phil Harris, Engility Corp.

Figure 2. Conceptual View a Managed Access System RAN Signal Coverage

Figure 2 and **Error! Reference source not found.** show managed access network RAN signal coverage. It is designed to overwhelm signals from nearby commercial network towers (i.e., nearby carrier RANs). A simplified way to envision this is to think about managed access RAN signal coverage as a cloud of radio energy that sits between illegal cellular devices and nearby commercial cellular networks. Commercial network RAN signals are overwhelmed by signals from the managed access system RAN. Cellular devices operating within the managed access RAN connect to the managed access cellular network; this is analogous to, but not quite

technically the same as, roaming processes that routinely occur between commercial cellular networks.



Source: Phil Harris, Engility Corp.

Figure 3. Conceptual View Managed Access RAN Signal Coverage Underlay

With managed access, a cellular device connects to the managed access RAN as if it were part of a commercial carrier's network. Once a cellular device is captured by a managed access system, unique identifying information retrieved from the device is compared against a list of known authorized devices. An authorized list is commonly referred to as a "white list". If a device is documented on a white list (indicating system operator authorization) the MAS will re-

direct that device to the commercial network for call completion. If a device is not authorized and included on the list, then service requests to or from a captured device are denied.

In managed access all connected devices are, by definition, assumed to be contraband and blocked by default. Authorized handsets appear on an exception list called a "white-list." Conversely, commercial carriers employ "black-lists" by to deny service to specific handsets, assuming all other connected cellular devices are authorized by default (assuming a valid cellular service agreement is in place.)

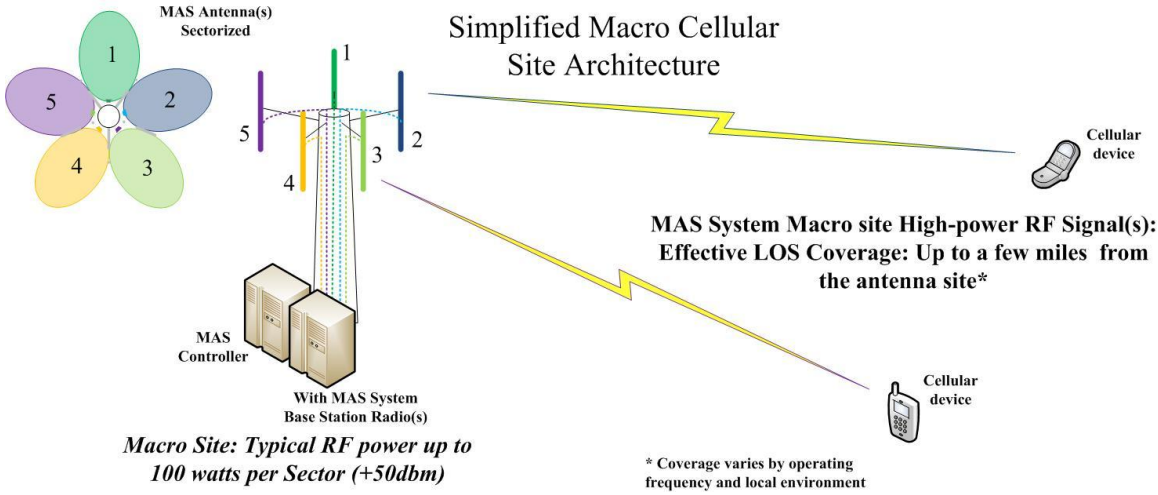
Managed access system technology-related choices are important. Regardless of the underlying wireless technology used to provide managed access RAN signal coverage, once a device is captured managed access network processes mitigate access to cellular services. Disposition of wireless service requests associated with devices falling under the control of any managed access network is dependent on MAS functions riding atop the RAN. Correctional facility policies, regulations, and guidelines ultimately define how a MAS operates.

MAS Architecture: Macro versus Small Cells versus DAS

Effective managed access RAN coverage, regardless of the underlying cellular technology, is critical to facilitate consistent capture of cellular devices. Managed access via DAS technology is presented to illustrate how DAS-based managed access contrasts with and complements traditional cellular macro-site and small cell technologies.

MAS RAN coverage throughout large open spaces can often be established using cellular topology based on a small number of relatively high-power base stations located in cell sites designed to provide coverage throughout a relatively large area (e.g., in a correctional facility located in a rural setting.) In a commercial network macro sites would be spaced to provide overlapping and continuous regional RAN coverage. This type of cell site technology is

categorized as "macro" cellular technology within this report. In this type of network, macro cellular sites may be supplemented by low-power, location-specific, repeaters and/or small cells which augment RAN coverage within specific buildings or outdoor areas.

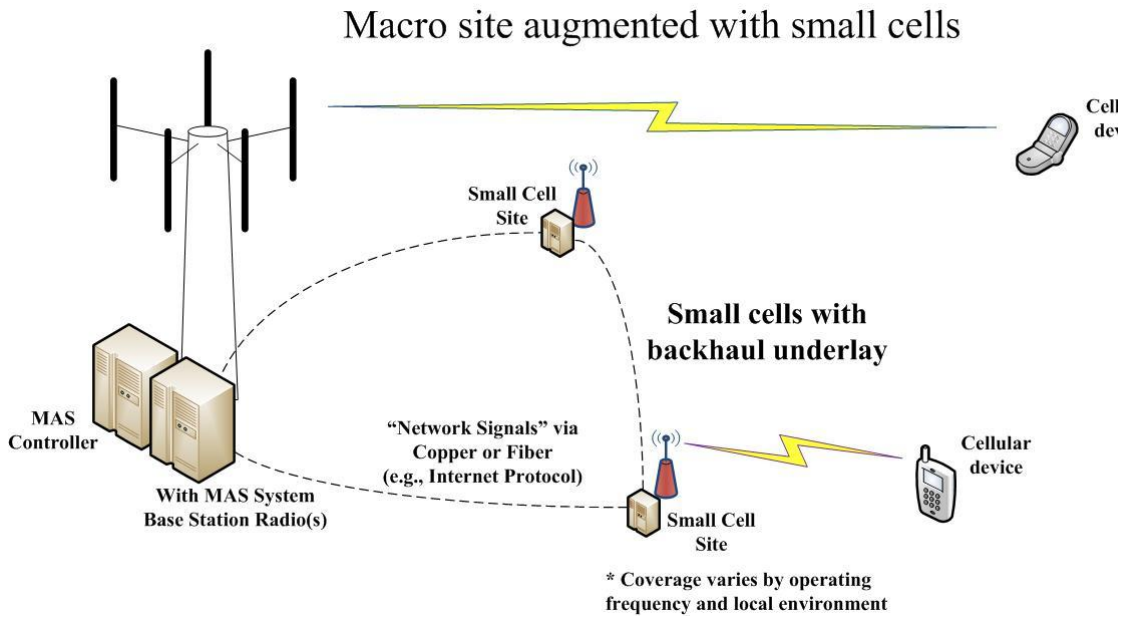


Source: Phil Harris, Engility Corp.

Figure 4. Traditional Macro Cellular Site

Figure 4 shows an example traditional macro cellular site that utilizes a sectorized antenna system (directional antennas each fed by a radio operating on a discrete frequency). Commercial cellular RANs are comprised of many (hundreds/thousands) of similar sites optimized for specific coverage and frequency re-use requirements. Commercial cellular networks use macro cell sites that support mobility so that cellular handsets can be "handed-off" between cellular base stations while maintaining service while users move throughout the network coverage area.

Use of a macro cellular architecture for a managed access RAN is suitable for some applications, but it presents coverage challenges for managed access deployments in correctional institutions located in a densely populated urban environment or for institutions that have a relatively small (or otherwise constrained) footprint. An alternative approach, for this type of constrained environment, is to establish managed RAN coverage via distributed antenna and/or



Source: Phil Harris, Engility Corp.

Figure 5. Small Cells Augmenting Macro Network RAN Coverage

small cell technology. Unlike macro sites, RANs established with distributed antenna and small cell technologies (shown in Figure 5) rely on small antenna systems and relatively low power transmitters.[19]

Use of DAS technology within a MAS architecture provides the ability to finely tailor (or augment) RAN network coverage in support of constrained functional environments. Distributed antenna system technology is not unique to managed access; DAS technology is deployed by many commercial operators to augment RAN commercial networks, primarily as a tool to increase capacity or to improve network coverage within specific venues such as office buildings, shopping centers or sports complexes where macro network coverage is inadequate. Low-power DAS and small cell technologies are also becoming increasingly relevant for

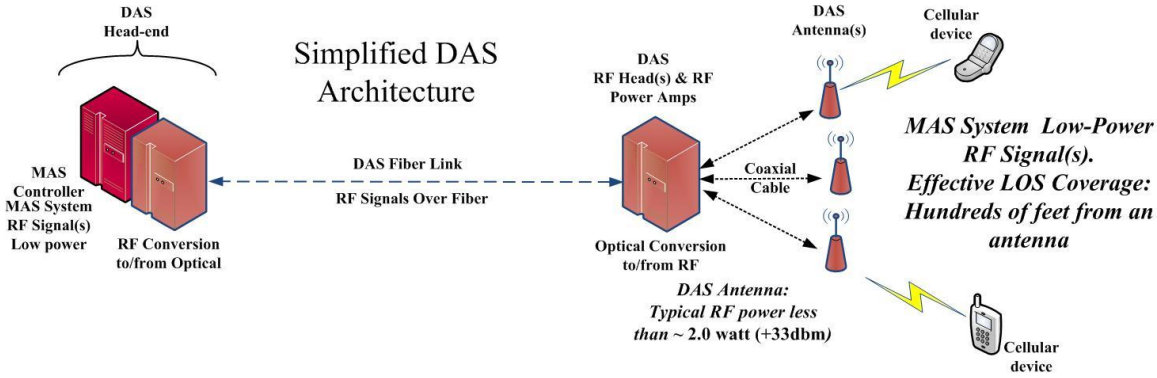
[19] Small cell technology is described here to be analogous to DAS in terms of signal coverage, and certainly analogous to distributed antenna technology from the perspective of physical plant requirements. Small cells are not part of the Baltimore deployment, and at the time of this report the authors were not aware of MAS products based on small cell technology. Small cell technology is acknowledged in this report because the technology is becoming an increasingly prevalent within commercial cellular network operations. Understanding the difference between the two technologies clarifies how DAS technology is unique.

commercial operations in densely populated urban areas where frequency re-use in the RAN has become important tool to increase network density and improve network capacity. Network RAN designs based on distributed antenna and small cell technologies, for both managed access and commercial networks, are highly dependent upon the specific venue where they are deployed.

DAS technology and small cell technology are often interchangeable because, from a user's perspective, network services provided through them are indistinguishable. Setting coverage similarities aside, there are significant architectural differences between small cell and DAS technologies. The primary difference between small cell and distributed antenna technologies is how and where network signals and service data are processed within the cellular network. Radio antennas are used within the RAN to establish the wireless interface through the atmosphere by converting electrical signals (at radio frequencies) into electromagnetic waves which are transmitted into the atmosphere (and vice versa in the receive direction.) An important point, in context of DAS technology, is that all wireless signals including digital cellular network wireless signals are analog as they pass through an antenna system.

System and customer data in a small cell network is conveyed through the network, in digital format, all the way to the edge of the network where it is processed by a transceiver into an analog radio signal operating at the desired radio frequency for interaction with the an antenna system. In contrast to small cell technology, network signals in a (optical) DAS system are processed into analog electrical signals, at the RAN operating frequency, at a central location (often referred to as a DAS "head-end") where they are immediately converted from electrical to optical format for transport through fiber optic cable to/from a remote RF head location were the analog radio signal is converted back to an electrical signal at the desired RAN operating

frequency[20]. Figure 6 depicts an optical DAS system in context of managed access. A centrally located DAS "head-end" can feed multiple remote "RF heads" via optical fiber interconnections.



Source: Phil Harris, Engility Corp.

Figure 6. Distributed Antenna System Technology

Cellular communications are obviously bi-directional. In the network transmit (downlink) direction once converted back in to electrical format by the remote RF head, the analog radio signal can be further filtered and processed though an analog amplifier system before the signal is applied to an antenna. The receive (uplink) direction can also be filtered and amplified in a similar way at the remote RF head before conversion from electrical into optical format for transport to the central head end. Depending on system complexity and features, the final transmit power at each antenna can often be fine-tuned remotely to adjust RAN coverage. A prime benefit of DAS technology is that it facilitates centralization of many network functions at a single central location. Because all radio signal processing occurs at a central location, system components at the remote RF head are less complex, and technology upgrades can occur at the head-end location instead of upgrading multiple small cell radio components at remote antenna locations. With DAS the over-all system architecture is less complex. Remote upgrades (within

[20] Some DAS technology uses coaxial cable instead of fiber optic technology, eliminating the electro-optical conversion process. The use of coax includes cost and performance trade-offs that are beyond the scope of this report.

hardware limitations) may be implemented without being observed by inmates, resulting in a more secure and safer process.

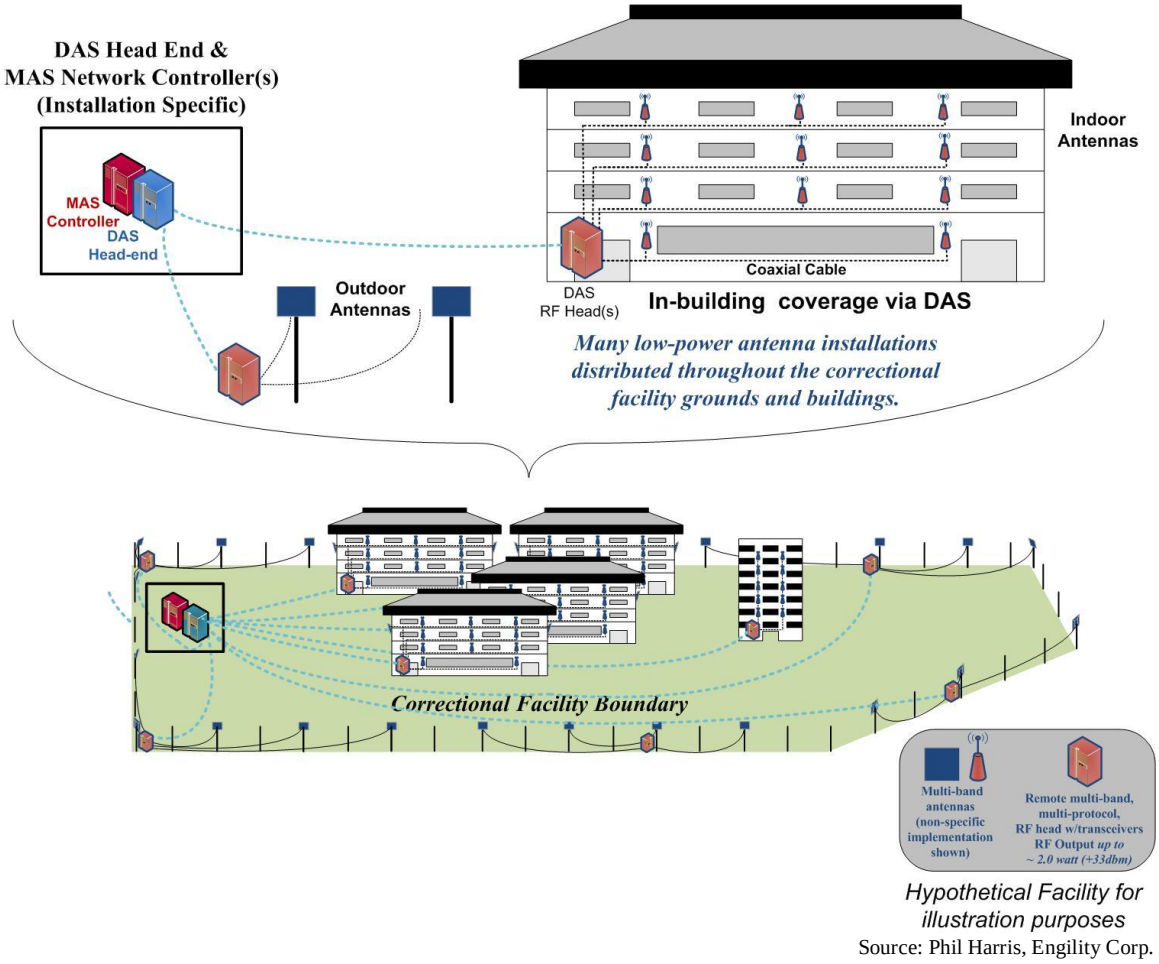
In a correctional facility managed access functionality, deployed atop DAS RAN technology, requires deployment of fiber optic cables to interconnect the DAS "head-end" with remote optical RF heads. AC Power must be provided at the DAS RF head location to support system telemetry, optical conversion and analog signal amplifiers. Antenna installation usually also requires relatively short coaxial cable runs from the remote RF head(s) to nearby antennas that are optimized for specific frequencies and RAN coverage goals (in some cases it may be useful to think of a single remote head supporting a cluster of nearby antennas.)

DAS deployment usually requires significant infrastructure costs. Logistical support required for the installation of conduit and associated hardware to support of any kind of cable-based signal distribution system is not insignificant, because it is usually "retrofitted" into an existing structure, or series of structures, not originally designed to accommodate it. Installation can involve deployment of extensive hardened cable raceways and/or electrical conduit designed to meet fire and electrical codes while protecting fragile optical and coaxial cables against vandalism. Antenna installations must also be hardened, and installed in a secure fashion. Installation of a DAS usually involves construction within spaces normally occupied by inmates[21].

Officials in Baltimore noted that inmates were able to sabotage the managed access system by damaging antennas in some locations even though they were installed on walls 15 to 20 feet above the floor. DAS components located in areas only accessible to staff members were also able to be sabotaged. DAS head end equipment, and remote optical radio heads must also be

[21] Note that this is equally true for any cable-based technology, to include DAS, distributed sensing, or distributed jamming technologies.

secured and protected. Remote management of all active MAS components is critical for diagnosis and understanding of system status prior to entering prisoner occupied areas.



Source: Phil Harris, Engility Corp.

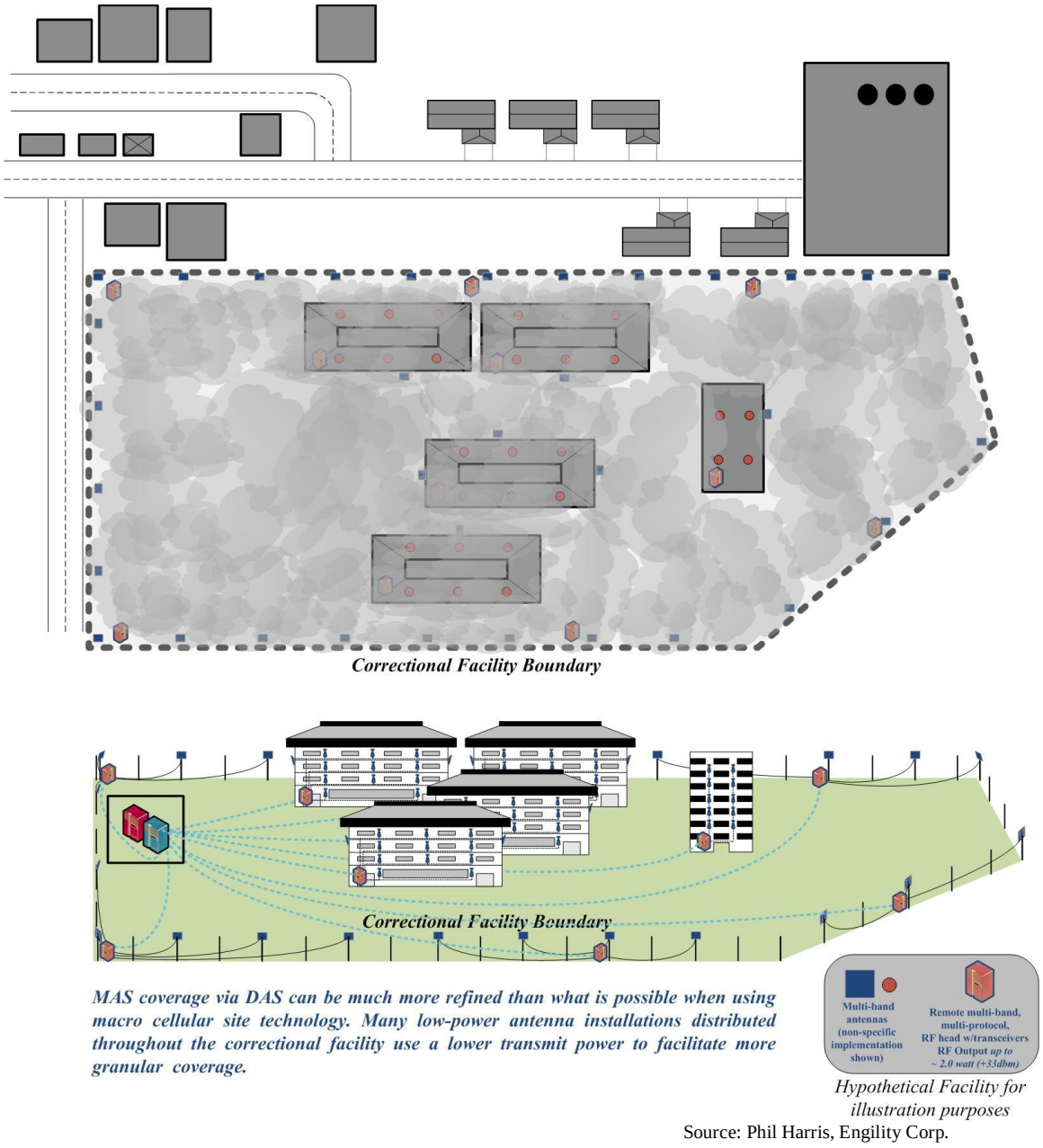
Figure 7. DAS for In-building & Outdoor RAN Coverage

Radio signals rapidly degrade in the atmosphere and the ability of a RAN network to present a dominant signal and maintain effectiveness decreases with increasing distance from a base station antenna. Simply increasing base station transmit power, or optimizing antenna orientation to increase coverage reaches a point of diminishing returns because maintaining desired coverage and effectiveness is a balancing process constrained by the legal obligation to constrain managed access system signals within authorized coverage boundaries. RAN coverage is optimized by carefully optimizing transmit signal power levels at the lease boundary perimeter against those received from nearby commercial networks. The result of this balancing act may be coverage

holes within the facility or within specific buildings where, for a number of reasons, commercial network signals remain dominant. Establishing ubiquitous coverage using macro technology can be complicated because prisons are made from materials that attenuate (block) and reflect RF signals in ways that are often impossible, or impractical to predict. For example, signals from a macro base station located on one side of a jailhouse may be attenuated enough by the building structure to allow an illegal cell phone to connect to a commercial network when used near the opposite side of the same building.

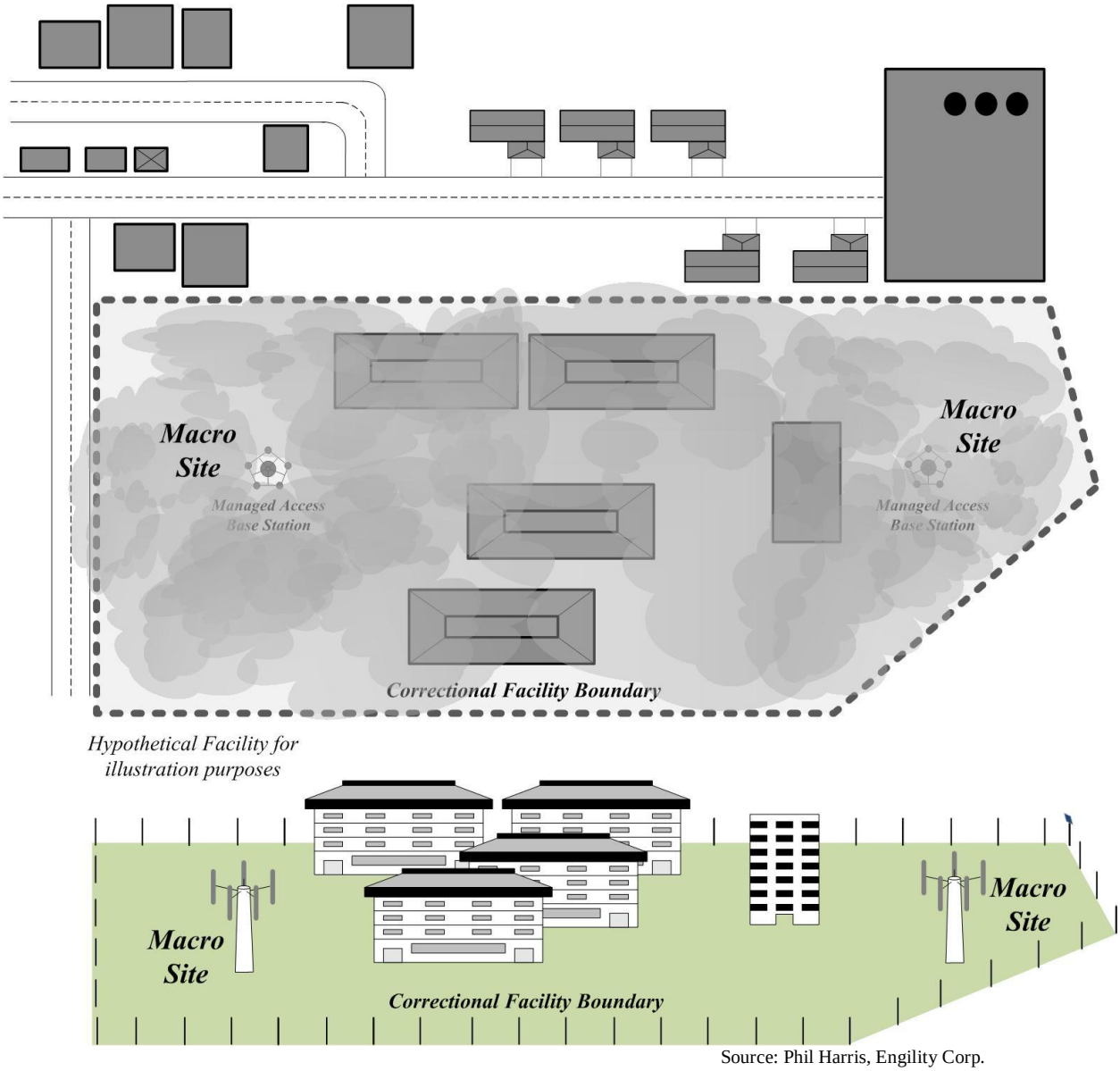
DAS based managed access technology utilizes a network of low-power antenna sites to establish an effective RAN signal throughout a correctional facility. DAS technology allows system operators to establish RAN coverage in a much more granular fashion.

For example, Figure 8 shows a hypothetical correctional facility using DAS technology with directional (e.g., flat panel) antennas around the perimeter of the facility. Antennas deployed in this way around the facility perimeter would focus RAN signal energy inward toward the controlled area, rather than outward in a transmission pattern typical for a centrally located macro antenna system (Figure 9.) The DAS example shown Figure 8 also includes antennas interior to compound buildings. This can be particularly helpful when dealing with irregular-shaped urban coverage areas because RAN coverage can be constrained to specific buildings, or within specific areas accessible to inmates; minimizing the need for the managed access RAN to blanket the entire facility.



Source: Phil Harris, Engility Corp.

Figure 8. MAS RAN coverage via Distributed Antenna technology



Source: Phil Harris, Engility Corp.

Figure 9. MAS RAN coverage via macro site technology

Rural (Macro) versus (Urban) DAS: A Real World Example

Figure 10 compares the relative coverage area and equipment density of a DAS-based network equipment in an urban setting (Baltimore, MD) to a macro type of installation in a rural location (Parchman, MS). The two areas shown in Figure 10 are scaled to emphasize the difference in size: the two DAS systems in Baltimore City Jail complex use nearly 500 antennas to achieve managed access coverage within a significantly smaller footprint when compared to

the system installed at MSP in Parchman. The Parchman RAN is designed to provide coverage for a significantly larger area, using a single macro cell site with a water tower mounted antenna system (Figure 11.) The Parchman MAS RAN coverage extends throughout an area of approximately four square miles, via a single macro site augmented with in-building repeaters for coverage inside specific buildings.[22] In contrast, the combined coverage of the two urban DAS-based systems in Baltimore cover approximately one million square feet of building space located within a single (~1200 x 1200 square foot) city block.

[22] Source: Tecore

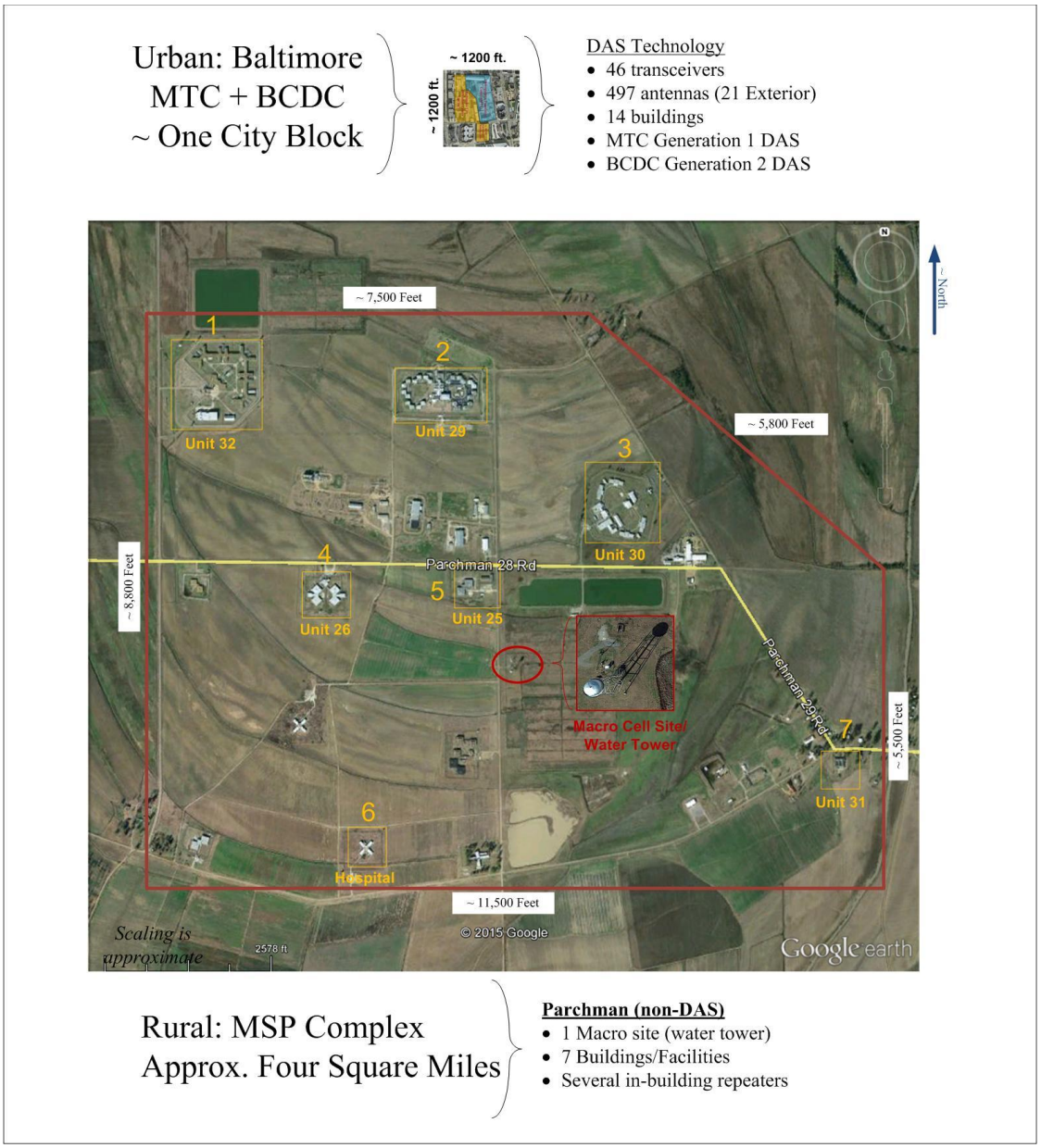


Image Source: Google Earth
Data Source: Tecore
Annotations: Phil Harris Engility Corporation

Figure 10. Urban/DAS in contrast to Rural/Macro based MAS

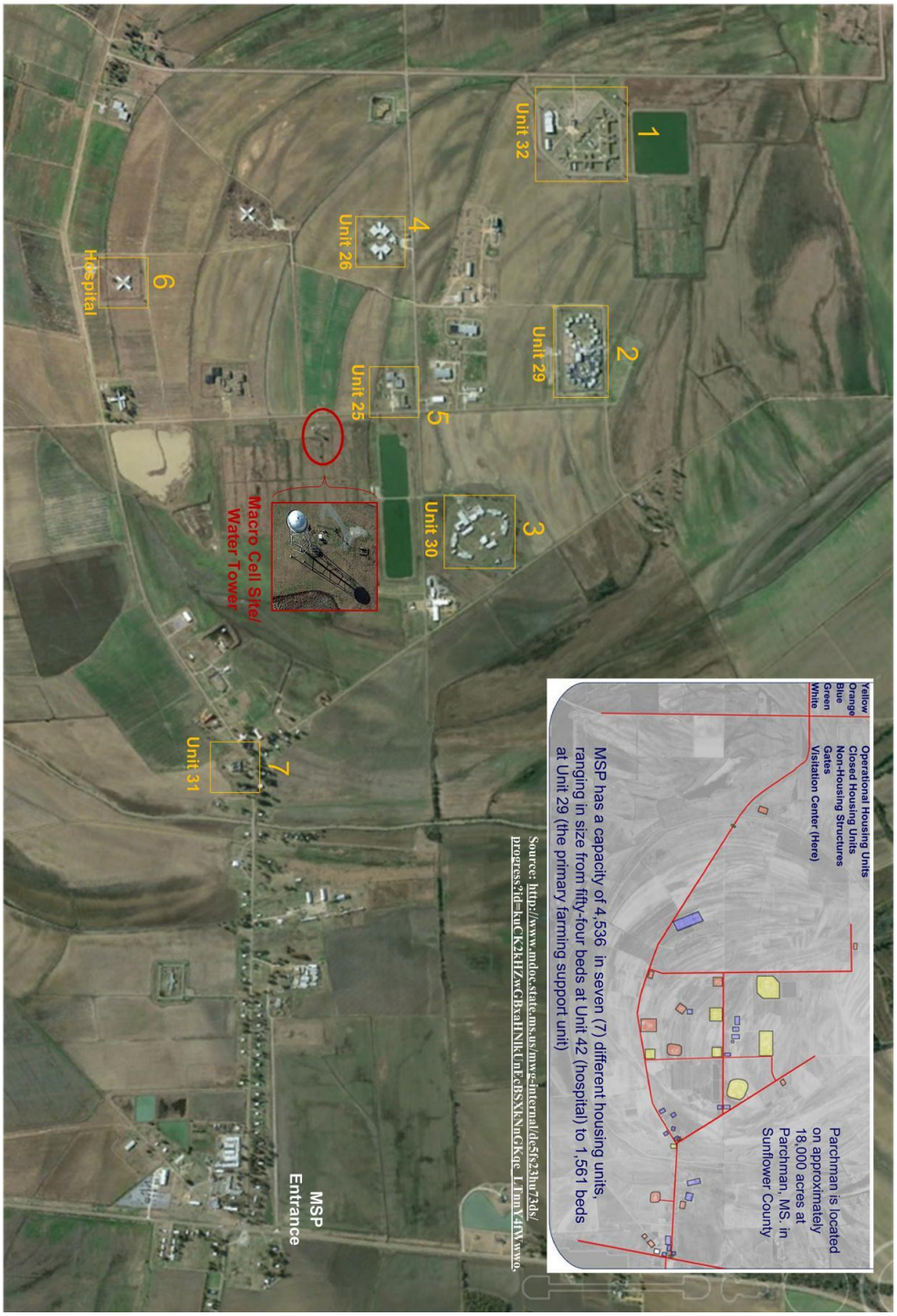


Image Source: Google Earth
Data Source: MSP
Annotations: Phil Harris Engility Corporation

Figure 11. MSP Parchman Complex and Surrounding Area

The DAS-based systems in Baltimore use a total of 46 transceivers feeding 496 antennas (475 interior + 21 exterior) to provide RAN coverage spanning 14 buildings (see Figure 12.)

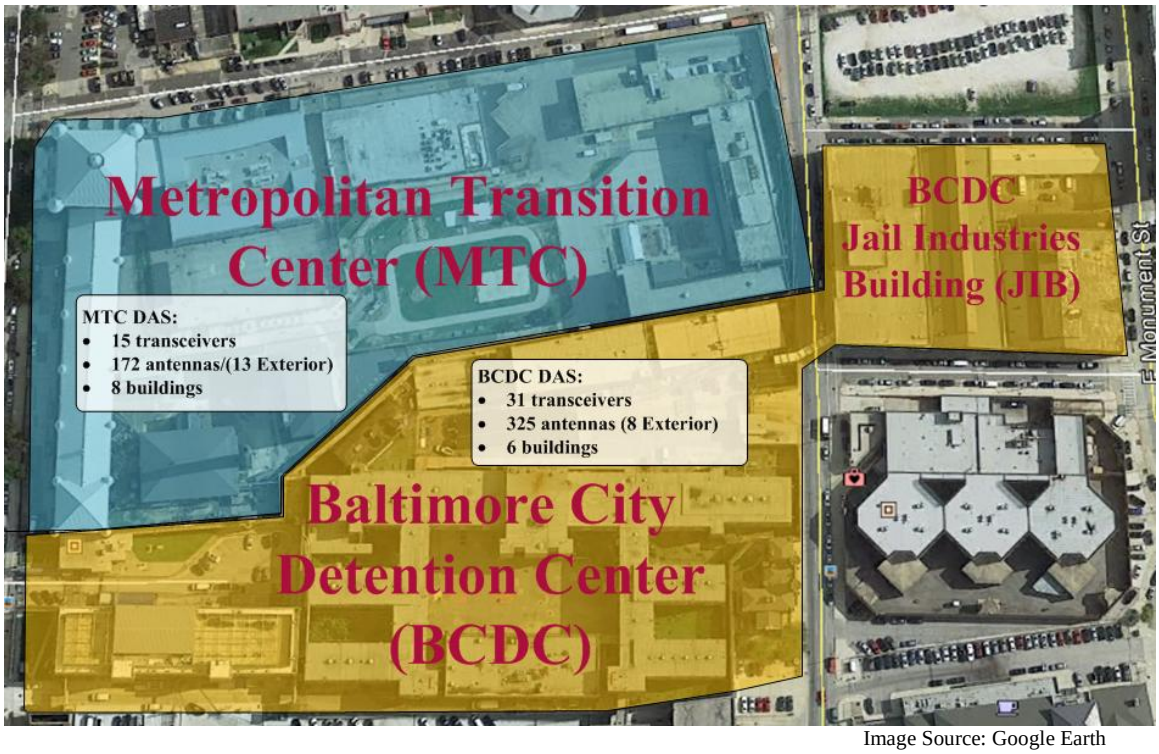
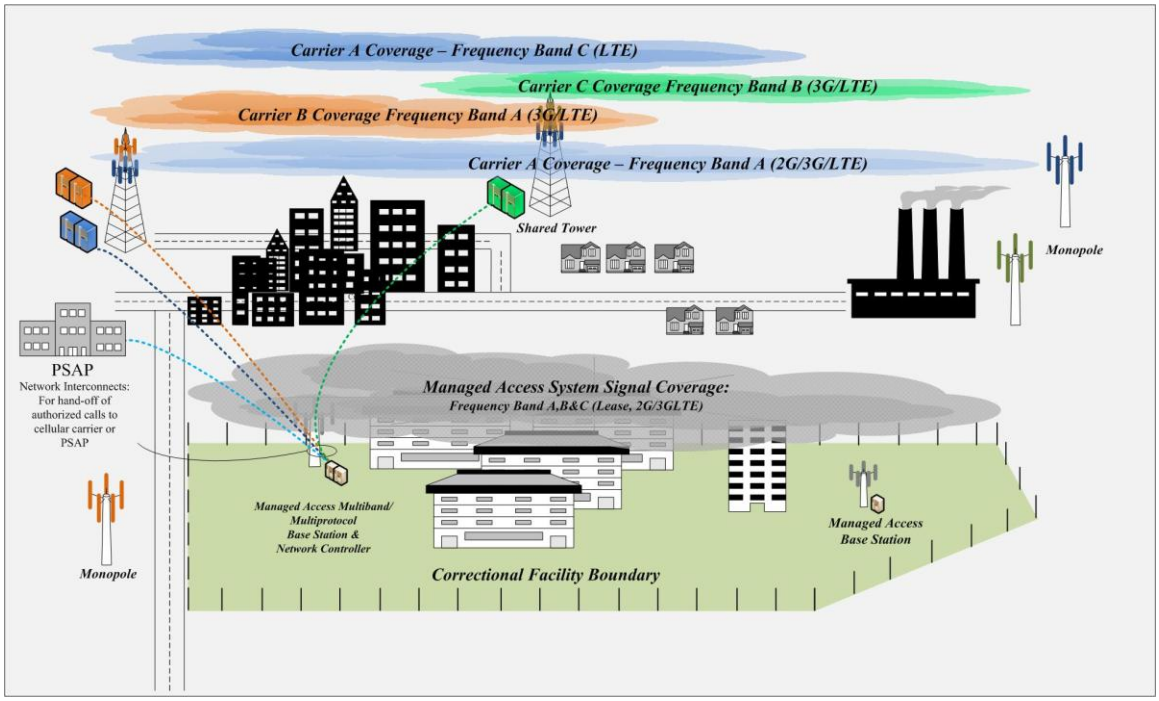


Image Source: Google Earth
Annotations: Phil Harris, Engility Corp
Tecore provided system data

Figure 12. Baltimore MTC and BCDC Managed Access Systems

System Interconnections: 911 and Other Authorized Calls

Procedures for handling of legitimate emergency service (911) call requests placed via the MAS will be dependent upon local agency MAS policy, state and local regulations, and FCC rules which legally define what a legitimate service request is. Depending on local policy, 911 calls may be triaged locally within the facility, routed directly to cellular carriers for further processing, or routed directly to an appropriate public safety answering points (PSAP). The latter case is how 911 calls are managed by the Mississippi State Penitentiary (MSP) in Parchman. In contrast to MSP, any 911 call processed by the MAS in Baltimore is routed to a correctional facility master control center for triage by correctional personnel.



Source: Phil Harris, Engility Corp.

Figure 13. Managed Access System and Cellular System Interconnections

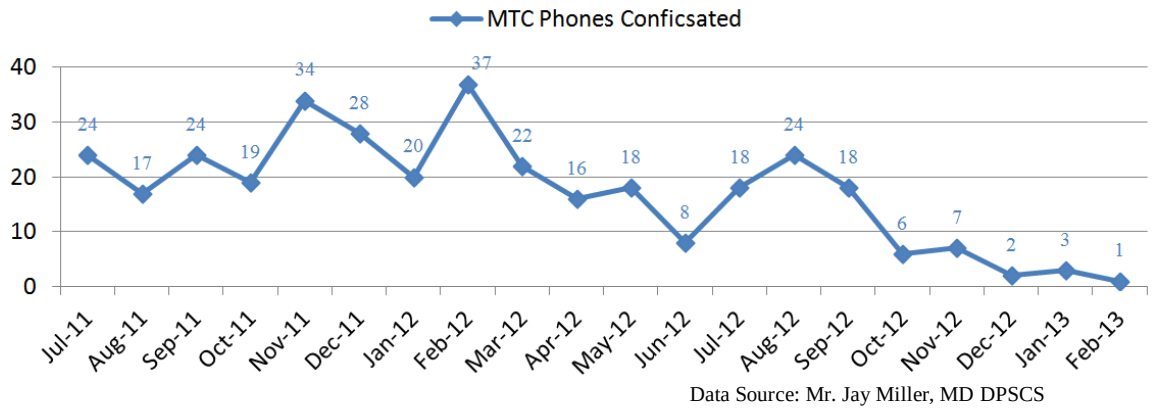
To directly route legitimate 911 calls to a nearby PSAP, network connectivity is required between the managed access network and nearby cellular carrier networks and/or directly to the local/regional PSAP. These interconnections are acknowledged and depicted in Figure 13. Implementation choices and the cost of these interconnections are subject to local requirements that define implementation choices and PSAP driven policies. It is important that MAS operators consider agency policies, physical implementation issues, and ongoing operation of any inter-network connections to ensure associated one-time and recurring operating costs are acknowledged.

Managed Access Technology at the Baltimore City Jail Complex

Officials from the Maryland Department of Public Safety and Correctional Services (DPSCS) indicated that the incentive for seeking a solution to illegal cell phone use within the Baltimore complex increased significantly following use of an illegal cell phone to arrange a

successful "hit" on a witness. This hit was arranged, or ordered, using an illegal cell phone within Baltimore City Detention Center (BCDC). DPSCS indicated that they were not entirely sure if managed access technology could be successfully deployed in the city. The MTC complex had a higher number of cell phone confiscations, and deployment of a system at the MTC was less complicated than it would be at BCDC, so DPSCS decided to deploy managed access at the MTC first. A managed access system was subsequently installed at BCDC in April 2013, as part of an emergency procurement following the indictment of 13 BCDC correctional officers for smuggling contraband.

Prior to deploying managed access in the Baltimore complex, traditional security practices were in place. For example, there are two points of entry to the BCDC facility: the main entrance/lobby for civilians/staff and a sally port for prisoner processing. The front lobby is the primary entry point for the facility. Metal detectors are used to screen visitors and employees at these entry points, in conjunction with physical searches, x-rays of incoming packages, and vehicle searches. All inmates are searched upon entry or exit to/from the facility. These security procedures remained in place when the managed access systems were installed.



Data Source: Mr. Jay Miller, MD DPSCS

Figure 14. MTC Cell Phone Confiscations July 2011 – February 2013

In general as noted in the number of illegal cellular devices confiscated at the MTC has declined, and data provided by DPSCS in February 2015 indicate that there had been no cell phone confiscations at that facility since April 2013.

Note that the annual fiscal year in Maryland runs from July 1– June 30, so FYTD, as of mid-January 2015, essentially covered a six and a half month period. Figure 17 and Figure 18 summarize the number of non-routine housing searches in the MTC and BCDC facilities for fiscal year 2010 through mid-January in 2015. These data suggest positive effect of managed access technology in regard to possession and use of illegal cellular devices.

MAS Deployment in Baltimore

Both the MTC and BCDC managed access systems utilize DAS technology. The system in the BCDC (yellow in Figure 1) is the newest/most recently installed and it is based on a more recent generation of DAS technology. Both systems were provided by the same manufacturer, Tecore. The two systems are separate and RAN coverage does not overlap, however there is a fiber optic control link between the two systems which provides redundancy in case of control system failure.

MTC Managed Access

The MTC complex (blue in Figure 1) is comprised of 15 transceivers and 172 antennas (including 13 outdoor antennas). It provides coverage for 8 buildings. The MTC managed access system was authorized under contract in April 2012 and activated a year later, in April 2013, following a 19 month purchase and deployment period[23].

- September 27, 2011: initial RFP was released.

[23] This timeline provided did not include time required to prepare and release an RFP process that initiated the procurement.

- October 12, 2011: a pre-proposal conference was held.
- November 9, 2011: proposals were submitted.
- February 2012: the Secretary approved the recommendation of award.
- April 18, 2012: the Board of Public Works approved the contract.
- April 19, 2013: Final acceptance testing completed.

In an April 2012 press release, the DPSCS announced that the state agreed to pay Tecore approximately $2 million dollars to install the MTC managed access system and following a 60-day trial evaluation, enter into a three year service contract. DPSCS budget documents indicate that approximately $600,000 of the MTC project funding was provided by the Federal government [24]. A press announcement indicated that if the MTC MAS deployment was successful other facilities would be considered for deployment.[25] All FCC and spectrum lease issues were handled by the system supplier and the MTC managed access system was activated in 2013 at a cost of approximately $2,000,000.[26]

BCDC Managed Access

In contrast to the MTC deployment, the BCDC managed access system is comprised of 31 transceivers, 325 antennas (including eight exterior) for coverage that encompasses six buildings. The BCDC deployment was accelerated and deployed via an emergency procurement process that was initiated on May 7, 2013. The BCDC managed access system was activated in 2014; system acceptance occurred on January 4th, 2014 following a deployment timeline of just under

[24] See http://www.dpscs.maryland.gov/publicinfo/news_stories/in_the_news/20120423c.shtml and http://mgaleg.maryland.gov/pubs/budgetfiscal/2015fy-budget-docs-operating-Q00-DPSCS-Overview.pdf
[25] See http://www.dpscs.maryland.gov/publicinfo/news_stories/in_the_news/20120420a.shtml
[26] See http://www.dpscs.maryland.gov/publicinfo/news_stories/in_the_news/20120420a.shtml

7 months. The system supplier handled all FCC/spectrum lease issues for this system as well. Funding for this system was included in a, $4,714,647, FY2014 deficiency allocation.[27]

DPSCS noted that the end date of the newer BCDC contract was aligned with the end date of the MTC contract so support for both systems can be renewed via a single competitively awarded service contract. DPSCS indicated that the initial period of performance for the MTC service contract will end in October, 2015. At the time of this report, the MD DPSCS was initiating the RFP process to procure ongoing maintenance of these two systems following the current end date.

System Testing and Operation

MAS RAN coverage related to spectrum lease compliance should be followed by performance related acceptance testing. This was accomplished by the system vendor and prison staff to check/validate RAN coverage using commercial cellular handsets. System performance acceptance criteria specified for the Baltimore facilities requires network coverage throughout 98% of defined points within the prison; a point is defined by a physical location, a commercial carrier, and a cellular technology. DPSCS indicated that staff members also conduct ongoing coverage testing on a monthly basis, using a defined grid pattern check and confirm coverage inside each facility. Staff members also make spot checks outside of buildings, but they generally do not conduct a comprehensive outdoor test. Tecore conducts tests outside each facility on a regular basis, and the commercial carriers can also test to verify that there is no RAN coverage outside the authorized managed access system footprint.

[27] This total also included funding to deploy video cameras at the Baltimore Central Booking and Intake Facility. No further breakdown of this total is noted. See http://mgaleg.maryland.gov/pubs/budgetfiscal/2015fy-budget-docs-operating-Q00-DPSCS-Overview.pdf

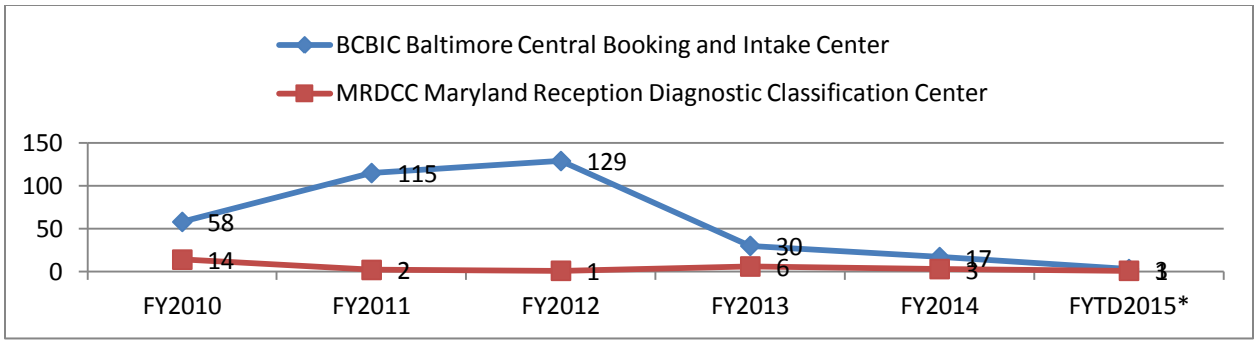
DPSCS noted that system complaints received were general in nature, and not related to specific calls being blocked. Since the BCDC was accepted, a DPSCS representative noted that he was only aware of one call incorrectly captured originating from a nearby legitimate user.[28]

DPSCS indicated that interaction with commercial carriers had been, in general, fairly smooth, stating that the major carriers (AT&T, Verizon, T-Mobile) have corporate managed access support units to interface with managed access vendor and correctional facility deployment teams. It was also noted that, for the most part, these support units are technical in nature and do not address policy or spectrum leasing issues. DPSCS also indicated that carriers do not provide much advance information about changes to their networks; therefore managed access system operators must continue to operate and manage their systems in a reactive rather than proactive posture. Both Baltimore MAS maintenance contracts require the system provider to upgrade the system in response to technology and/or coverage changes in the nearby commercial cellular environment.

BCBIC and MRDCC

Approximately $7.2 million in funding was allocated in the FY2015 DPSCS budget to deploy managed access technology at the BCBIC and MRDCC. This award, if placed, would extend managed access coverage to nearly all buildings within the Baltimore complex. As shown in Table 1 and Figure 15, the rate of illegal cell phone seizures in these facilities has fallen significantly without managed access technology in place.

[28] Two separate incidents were reported in the media shortly after the system was activated. See http://articles.baltimoresun.com/2014-02-09/news/bs-md-ci-jail-cellphone-blocking-issues-20140208_1_cell-phone-city-jail-tavon-white



*****Through January, 2015
Data Source: https://data.maryland.gov/Public-Safety/DPSCS-Data-Templates-Directory/rvm2-6rkn

Figure 15. BCBIC and MRDCC Cell Phone Seizures

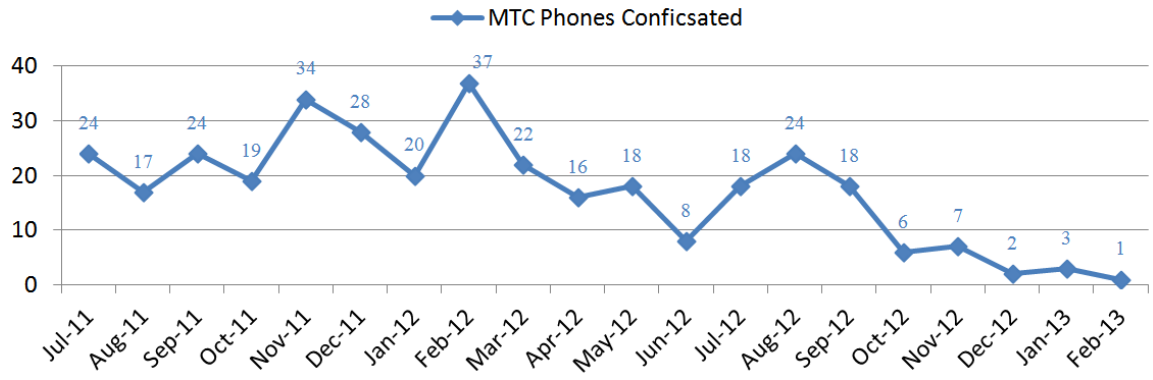
The (January 2015) DPSCS Fiscal 2016 budget overview indicates that funding for these systems has been eliminated:

> *"The department's fiscal 2015 appropriation includes nearly $7.2 million in general funds to implement cell phone managed access systems at the Baltimore Central Booking and Intake Center (BCBIC) and the Maryland Reception, Diagnostic, and Classification Center (MRDCC). Although the department had plans to expand implementation of managed cell phone access systems, which are already in place at the Metropolitan Transition Center and the BCDC, the fiscal 2016 allowance does not include funding for new systems. The department has not yet awarded a contract for the managed access systems at BCBIC or MRDCC.*[29]*"*

Conclusions

In general, as noted in Figure 16 the number of illegal cellular devices confiscated at the MTC has declined, and data provided by DPSCS in February 2015 indicate that there have been no cell phone confiscations at that facility since April 2013.

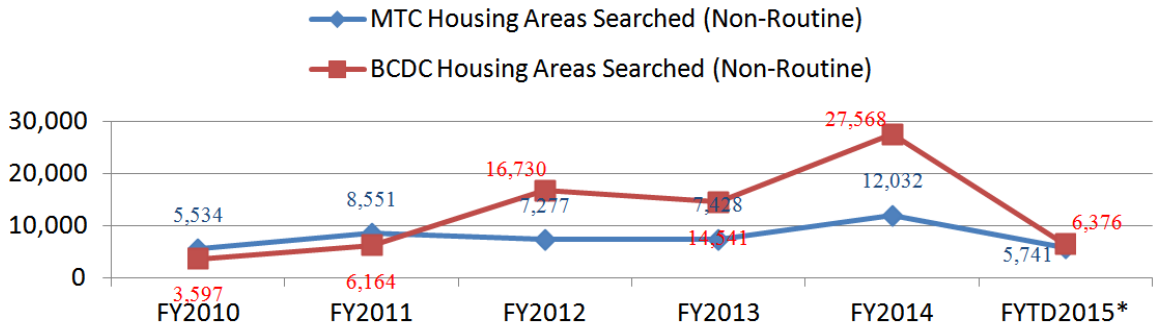
[29] See http://mgaleg.maryland.gov/pubs/budgetfiscal/2016fy-budget-docs-operating-Q00-DPSCS-Overview.pdf



Data Source: Mr. Jay Miller, MD DPSCS

Figure 16. MTC Cell Phone Confiscations July 2011 – Feb 2013

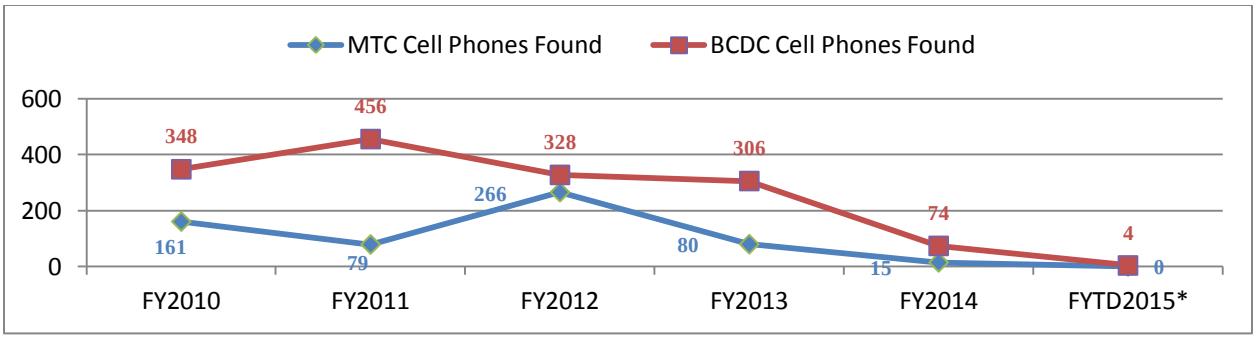
Figure 17 and Figure 18 summarize the number of non-routine housing searches in the MTC and BCDC facilities for fiscal year 2010 through mid-January in 2015. These data suggest a positive effect of managed access technology in regard to possession and use of illegal cellular devices. Figure 19 suggests that the availability of controlled dangerous substances also declined following the deployment on managed access technology.



*As of mid-January, 2015

Data Source: Mr. Jay Miller, MD DPSCS

Figure 17. MTC & BCDC Cell Phone Searches 2011 – 2015

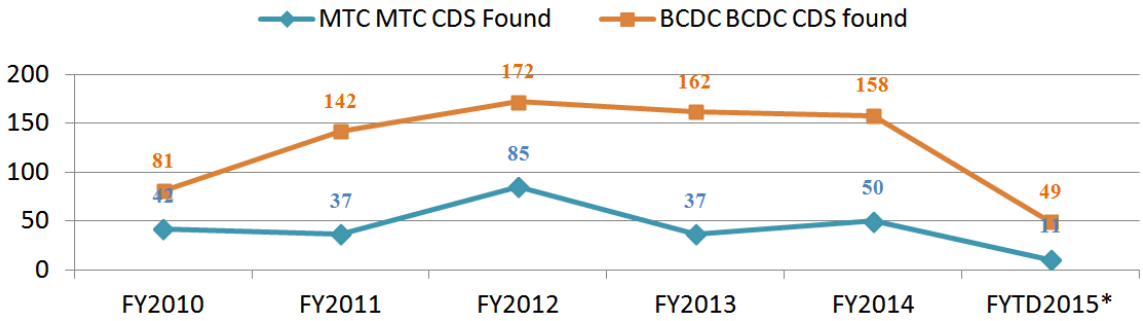


*Through January, 2015

Data Source: https://data.maryland.gov/Public-Safety/DPSCS-Data-Templates-Directory/rvm2-6rkn

Figure 18. MTC & BCDC Cell Phone Confiscations 2011 – 2015

Figure 19 suggests that the availability of controlled dangerous substances may have also declined following the deployment of managed access technology.



*As of mid-January, 2015

Data Source: Mr. Jay Miller, MD DPSCS

Figure 19. MTC & BCDC Controlled Dangerous Substances (CDS) 2011 – 2015

Data retrieved from publicly available Maryland Open Data Portal describes illegal cell phone seizure rates system-wide[30]. This data are summarized in Table 1 and they indicate that, system-wide, the rate of contraband Inmate cell phones found within Maryland correctional facilities has fallen in recent years. This trend is apparent both for facilities equipped with Managed Access technology as well as within facilities not equipped with the technology. A significant conclusion that can be made is that while managed access had a significant impact within the facilities where it was deployed, other factors unrelated to the technology such as policy changes also contributed to the overall decline of illegal cellphone use throughout the

[30] Data for each facility obtained via the Maryland Open Data Portal at https://data.maryland.gov/Public-Safety/DPSCS-Data-Templates-Directory/rvm2-6rkn. This data shown above was retrieved on July 1st, 2015.

prison system (to include faculties with deployed managed access systems). When queried about this overall trend system-wide, DPSCS suggested that increased vigilance implemented through policy changes, as well as increased mandatory penalties for those caught with an illegal device contributed to this reduction. For example, it was suggested that rotating correctional staff between regional prison entrance check points likely impacted the ability for staff members to smuggle in illegal devices. The consequences of possession of an illegal cellular device in a Maryland correctional facility have changed to now include criminal penalties, via misdemeanor charges which can result in up to a 3 year jail sentence. It was also noted that administrative sanctions that can now be levied against prisoners, to include disciplinary segregation and loss of privileges.

Table 1. DPSCS System-Wide Reported Contraband Cell Phones Found

DPSCS Reported Region totals: Contraband Found - Cell Phones	Total Cell Phones Found						Year to Year Change				
	(7/1/09-6/30/10)	(7/1/10-6/30/11)	(7/1/11-6/30/12)	(7/1/12-6/30/13)	(7/1/13-6/30/14)	2015 (7/1/14-1/30/15)	2010-2011	2011-2012	2012-2013	2013-2014	2015 (7/1/14-1/30/15
Department-wide	1098	1307	1303	870	281	97	209	-4	-433	-589	-184
North Region Totals	55	24	80	38	44	25	-31	56	-42	6	-19
South Region Totals	259	395	365	357	119	51	136	-30	-8	-238	-68
Central Region Corrections Totals	359	259	373	119	23	9	-100	114	-254	-96	-14
Central Region Detention Totals	425	629	485	356	95	12	204	-144	-129	-261	-83
DPSCS Reported Facility-Specific Contraband Found - Cell Phones	Total Cell Phones Found						Year to Year Change				
	(7/1/09-6/30/10)	(7/1/10-6/30/11)	(7/1/11-6/30/12)	(7/1/12-6/30/13)	(7/1/13-6/30/14)	2015 (7/1/14-1/30/15)	2010-2011	2011-2012	2012-2013	2013-2014	2015 (7/1/14-1/30/15
BCCC Baltimore City Correctional Center	158	164	99	8	3	4	6	-65	-91	-5	1
BCBIC Baltimore Central Booking and Intake Center	58	115	129	30	17	3	57	14	-99	-13	-14
BCDC Baltimore City Detention Center (Managed Access in operation)	348	456	328	306	74	4	108	-128	-22	-232	-70
BCF Brockbridge Correctional Facility	148	267	183	99	10	2	119	-84	-84	-89	-8
BPRU Baltimore Pre-Release Unit	22	6	3	7	0	1	-16	-3	4	-7	1
CDF Chesapeake Detention Facility	19	58	28	20	4	5	39	-30	-8	-16	1
CMCF Central Maryland Correctional Facility	2	4	3	18	2	3	2	-1	15	-16	1
DRCF Dorsey Run Correctional Facility*	n/a	n/a	n/a	n/a	1	9	n/a	n/a	n/a	n/a	8
ECI-A Eastern Correctional Institution Annex	2	3	1	0	0	0	1	-2	-1	0	0
ECI Eastern Correctional Institution	1	2	1	4	2	0	1	-1	3	-2	-2
EPRU Eastern Pre-Release Unit	3	2	1	6	3	1	-1	-1	5	-3	-2
JCI Jessup Correctional Institution	34	6	12	23	28	8	-28	6	11	5	-20
JPRU Jessup Pre-Release Unit*	7	41	137	194	12	n/a	34	96	57	-182	n/a
MCI-H Maryland Correctional Institution Hagerstown	2	8	12	0	17	9	6	4	-12	17	-8
MCI-J Maryland Correctional Institution Jessup	15	23	18	12	30	19	8	-5	-6	18	-11
MCI-W Maryland Correctional Institution for Women	0	0	1	0	0	0	0	1	-1	0	0
MCTC Maryland Correctional Training Center	3	4	9	4	4	11	1	5	-5	0	7
MRDCC Maryland Reception Diagnostic Classificatic	14	2	1	6	3	1	-12	-1	5	-3	-2
MTC Metropolitan Transition Center (Managed Access in operation)	161	79	266	80	15	0	-82	187	-186	-65	-15
NBCI North Branch Correctional Institution	2	0	1	0	5	0	-2	1	-1	5	-5
PATX Patuxent Institution	16	5	25	19	11	0	-11	20	-6	-8	-11
PHPRU Poplar Hill Pre-Release Unit	10	18	2	0	7	1	8	-16	-2	7	-6
RCI Roxbury Correctional Institution	18	3	3	5	3	2	-15	0	2	-2	-1
SMPRU Southern Maryland Pre-Release Unit	39	33	9	19	26	11	-6	-24	10	7	-15
WCI Western_Correctional_Institution	14	4	30	10	4	3	-10	26	-20	-6	-1

*Note: 12/13: All JPRU inmates were transferred to the newly opened DRCF (Dorsey Run Correctional Facility)
Data source: https://data.maryland.gov/Public-Safety/DPSCS-Data-Templates-Directory/rvm2-6rkn

A paragraph in the 2016 DPSCS budget document suggests the deployment of managed access technology deployment is complementary to other methods such as the recovery of contraband via canine unit searches:

"The department reports the rate of items found per 100 scans conducted by the Canine Unit. Between fiscal 2011 and 2013, the overall rate of contraband finds decreased from 1.34 to 0.42 items per 100 scans. However, the rate of contraband finds increased

significantly in fiscal 2014, to 0.93 items per 100 scans overall. The majority of items found in fiscal 2014 were weapons and drugs. The department attributes the increased finds to enhanced search techniques and increased use of intelligence and phone monitoring capabilities, which have allowed the Canine Unit to conduct fewer scans leading to an increased number of recoveries. ***The rate of cell phone finds remained stable in fiscal 2014 at 0.07 per 100 scans. As was to be expected, the rate of cell phone finds declined in the Central Region from 0.33 in fiscal 2013 to 0.13 in fiscal 2014 as a result of implementation of managed access systems at Baltimore facilities***[31]

In addition to the observations noted above, the following conclusions can also be made:

- As noted in the report about the rural system deployed in Parchman MS, good working relationships with nearby cellular carriers is critical. In Baltimore, the system vendor is responsible to maintain this responsibility, and this relationship is enforced in the service contract.
- MAS can effectively be implemented in an urban setting. Technology such as Distributed Antenna Systems (DAS) allows operators to refine and control system coverage within tightly constrained environments.
- DAS deployment is heavily reliant upon physical installation of cable, conduits and other supporting infrastructure. While this can be a challenging and costly task for any pre-existing facility, retrofitting an existing correctional structure is particularly challenging. Deployment of technology in a correctional environment creates unique logistical challenges involved with deploying it in areas where inmates reside and securing the system infrastructure from sabotage.

[31] See Page 11: http://mgaleg.maryland.gov/pubs/budgetfiscal/2016fy-budget-docs-operating-Q00Q-DPSCS-Operations.pdf

Finally, note that cellular devices are becoming more complex and multi-function in nature and, as a result they present an increasing number of threats based on capabilities other than communication via cellular telephony. Cellular managed access technology only addresses cellular communications capabilities and cannot, for instance, prevent use of non-cellular wireless capabilities, such as Wi-Fi, stand-alone computing or photographic capabilities which have become standard features in modern cellular devices. Managed access simply mitigates the connection of cellular radio transmissions between a handset and an external (e.g., commercial) network. Elimination of cellular communications capabilities makes other features present in these devices less useful to the inmates that possess them.

Appendix A: Examples of Contraband Cell Phone Activity

Contraband cell phones have been used for a variety of criminal activities inside and outside correctional facilities. While specific estimates of such activity have not been routinely collected or published, there is significant body of anecdotal evidence that the problem is widespread and continues to pose a public safety problem. Table 2 illustrates some recent examples of alleged or noted criminal activities that have been associated with inmate use of contraband cell phones.

Table 2. Examples of Contraband Cell Phone Criminal Activity

State/ Country	Report	Criminal Act(s) Noted	Inside or outside prison	Reference URL
South Carolina	2010	Murder (attempted)	Outside	http://newsone.com/753345/prisoner-ordered-hit-outside-of-prison-with-smuggled-cell-phone/
Georgia	2011	Organized Inmate Uprisings	Inside	http://www.valdostadailytimes.com/local/x1331361164/Cell-phones-spark-Georgia-prison-unrest
North Carolina	2012	Kidnapping & Harass-ment	Outside	http://www.newsobserver.com/2014/04/11/3776630/kelvin-melton-imprisoned-for-life.html and/or http://www.theguardian.com/world/2014/apr/12/north-carolina-inmate-kidnapping-mobile-phone
Ohio (other locations mentioned)	2012	Multiple	Inside/ Outside	http://www.springfieldnewssun.com/news/news/cellphones-weapons-and-drugs-flood-ohio-prisons-1/nMySK/
South Carolina	2012	Smuggling, blackmail, harassment	Inside/ Outside	http://www.postandcourier.com/article/20120430/PC16/120439959 and http://www.postandcourier.com/article/20120430/PC16/120439971
Georgia	2013	Planning Violent Robberies	Outside	http://www.wsbtv.com/news/news/local/inmate-accused-planning-violent-crimes-prison/nXbw8/
Georgia	2013	Homicide	Inside	http://chronicle.augusta.com/news/2013-03-24/gangs-cell-phones-blamed-rise-homicides-georgia-prisons
Indiana	2013	Harassment	Outside	http://www.theindychannel.com/news/call-6-investigators/families-victims-targeted-by-indiana-state-prisoners-with-illegal-phones
Tennessee	2013	"violent crimes"	Outside	http://www.newschannel5.com/story/23631961/prisoners-confiscated-cell-phones-help-non-profit

State/ Country	Report	Criminal Act(s) Noted	Inside or outside prison	Reference URL
Georgia	2013	Prison Brawl Video	Inside	http://www.youtube.com/watch?v=C77wyuzh3oM
California	2014	Drug Trafficking & Violent Crime	Outside	http://abc30.com/archive/9531064/
Maryland (Baltimore is mentioned)	2014	Smuggling etc.	Inside/ Outside	http://www.city-journal.org/2014/24_2_baltimore-correctional-services-corruption.html
Florida (other locations mentioned)	2014	Multiple	Inside/ Outside	http://tbo.com/news/crime/prisoners-use-of-smuggled-cellphones-on-rise-20140216/
Florida, Georgia (and other locations)	2014	Multiple	Inside/ Outside	http://www.nbcnews.com/news/us-news/cell-phones-n327311
Georgia	2015	Extortion	Inside/ Outside	http://chronicle.augusta.com/latest-news/2015-03-31/augusta-man-shown-beaten-leashed-prison-cellphone-photo
International				
Brazil (Baltimore is mentioned)	2014	Murder	Outside	http://www.firstthings.com/web-exclusives/2014/04/prisoners-are-calling-whos-answering
Honduras	2014	Extortion	Outside	http://dialogo-americas.com/en_GB/articles/rmisa/features/regional_news/2014/05/30/honduras-seguridad

Appendix B: Managed Access Technology

Cellular Telephony

The material in this section consists of background information originally included in the unpublished Parchman report. This information is included here as a supplementary technical overview of managed access technology operations.

Cellular telephony, as a wireless radio service, functions much like other radio technologies. Radio technology, when boiled down to bare essentials, involves a process of inserting (modulating) information of various forms onto a radio signal which utilizes radio frequency energy to convey the information through the environment wirelessly. As this wireless energy transits through the atmosphere and surrounding environment some level of radio signal degradation occurs prior to reaching a receiver. This degradation is expected and attributed to a number of predictable and/or unpredictable factors. When the signal arrives at an antenna intact, a receiver converts the information back into a format useful for its intended purpose: this process is called demodulation. Protocols and procedures are used to process (modulate/demodulate) information during wireless transmission, using specific radio frequencies to support the transmission. Some receive processes are based on open standards and others use proprietary technologies. Specific engineering and business needs drive how radio access network (RAN) systems are developed and deployed. For example, commercial carriers Verizon, Sprint, and AT&T each use RAN technologies based on 3GPP LTE standards, but their RAN interfaces are different in many ways, and therefore non-interoperable because of specific implementation choices.

Cellular network operators are authorized via Federal Communications Commission (FCC) licenses to use specific radio spectrum frequencies throughout defined geographical areas.

Licenses are often granted following successful bids levied in a spectrum auction, often at costs to a carrier measured in billions of dollars. In exchange for the proceeds received from winning auction bids, the FCC grants the winning carrier exclusive use of frequencies in defined areas so they can invest in RAN infrastructure in a predicable way to provide customer services in the most optimal way suitable to their business plans. They can do what they want and need to, as long as they do not exceed the technical and regulatory limitations associated with their FCC authorizations. Exclusivity means that commercial carriers retain sole legal access to authorized spectrum; a right that operators defend vigorously.[32] Any unauthorized signals emitted in carrier controlled spectrum space are considered to be interference by the carrier and the FCC. Managed access, considered as a category of technology (rather than a specific vendor product) operates as a tenant using carrier RAN frequencies. This spectrum lease process requires close coordination between MAS operators and carriers to ensure systems operate in a legal manner.

For readers who are unfamiliar with wireless cellular technology, it is important to understand that there are constraints related to how wireless systems are designed and how they operate. Subtle details are significant when considered in context of how RAN coverage is established and maintained. Many radio technologies, such as land mobile radios, are designed to operate in relatively quiet and interference/noise-free wireless environments. These radio services are typically designed to function with relatively few high-powered transmitters using antennas mounted atop tall towers to create networks engineered to operate in a relatively uncluttered radio environment. This type of network provides efficient signal coverage

[32] There are a number of Federal proceedings underway that are investigating ways to "share" spectrum, with a goal to more efficiently utilize limited spectrum resources. For example, FCC Docket GN 13-185, Regard to Commercial Operations in the 1695-1710 MHz, 1755-1780 MHz, and 2155-2180 MHz bands, is examining approaches to sharing spectrum between commercial and federal users; Docket GN 12-354 is considering commercial operations in the range of 3550-3650 MHz, currently used by federal users.. If these efforts are successful, and commercial carriers are allowed access to new spectrum resources, or other spectrum users are allowed shared access to cellular frequencies, the technical implications facing managed access technology may become very complicated.

throughout an area using the fewest number of network sites and the minimal amount of supporting infrastructure (i.e., additional base stations/repeaters). This type of technology is often referred to as "noise-limited".

Commercial cellular radio infrastructure can be characterized by a few key distinguishing characteristics:

1. Cellular networks, similar to trunked land mobile radio technology, are bifurcated, composed of a wireless customer air interface between the customer and the carrier network, often referred to as the "radio access network, or RAN". A second, carrier backbone network, is also established for interconnect cellular towers and to connect customers to off-network services.

2. A typical commercial cellular network is comprised of a relatively large number of base stations designed with relatively low profile towers, densely spaced in a way to efficiently support the greatest number of connections (i.e., users) via the RAN and/or to convey the largest amount of data through the access network. Cellular operators route customer traffic through their network backbone using back-haul connections (e.g., microwave radio, fiber optic cable, copper cable);

3. Cellular technology, similar to land mobile radio, must support customer mobility. Cellular networks are designed to support the movement of large numbers of relatively low-powered user devices between cell towers that make up the RAN, while maintaining network and data connections, and;

4. Cellular RAN's are constructed using a defined set of radio frequencies with a high level of frequency re-use and efficiency (i.e., using the same frequency resources over and over again).

Because of the high level of frequency re-use, cellular technologies are designed to operate amid a relatively high level of radio interference created by adjacent cell sites. This is referred to as an "interference-limited" RF environment, whereby a baseline level of signal interference is expected in exchange for increased levels of spectrum re-use and spectrum efficiency, resulting in the greatest rate of return on a carrier's investment. Cellular base station density varies by business needs and typically mirrors the number of potential cellular customers; thus the number of base stations in an urban setting is typically greater and more densely deployed than the number of base stations in a rural setting where potential rate of return on investment is significantly less.

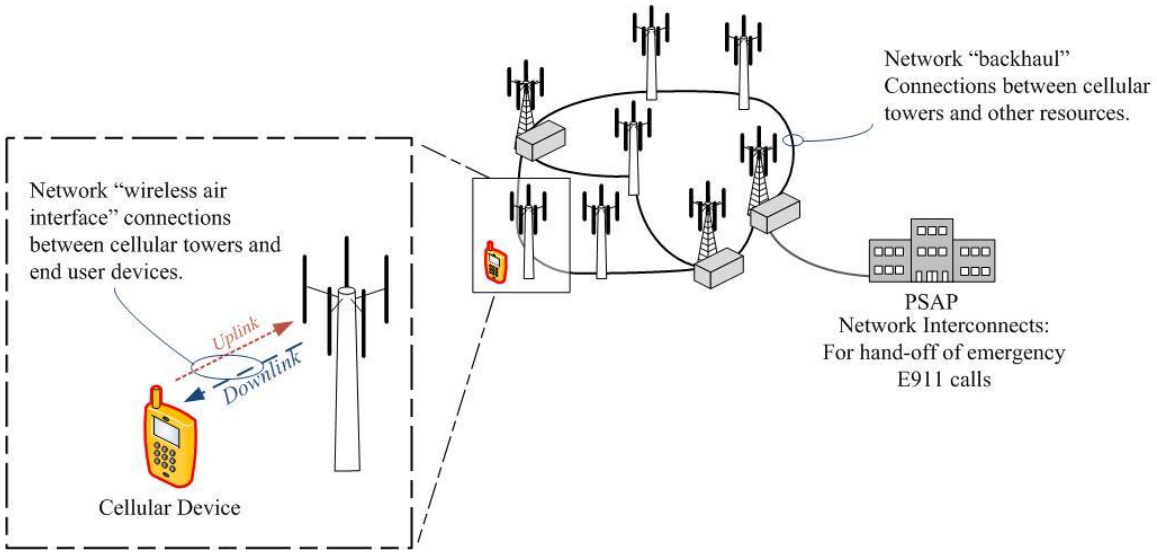
In a cellular environment, as with land mobile radio, wireless transmission occurs in two directions. Cellular transmissions from a base station radio transmitter directed to receiver components within portable cellular device are typically described as "downlink" transmissions. A transmission in the reverse direction, originating from a relatively low-powered end user device (e.g., cell phone) towards a base station receiver, is often referred to as an "uplink" connection. In a cellular network, the constraining wireless link is usually the uplink from a low-powered end-user device. If either the downlink or uplink connection fails, or becomes interrupted, then communications services requested by the cellular device user will not work.

To combat illegal cell phone use, both managed access and jamming technologies rely on highly engineered systems to provide radio frequency signal coverage using cellular network access frequencies. However, there is a significant difference in how this coverage is used is

used. For example, jamming technology disrupts the communications path between the user and the network. Managed access does not, it depends on establishing successful communications between the network and cellular device to capture a wireless device and then use of network control to selectively grant or deny requested network services.

Managed Access

A managed access system is, fundamentally, a cellular network with limited scope and reach. A managed access network is designed to present the "dominant" network signal within its limited authorized RAN coverage area. Managed access networks are designed to operate using the same frequencies and protocols as those used in the RAN of nearby commercial cellular carriers. Cellular devices work by listening for a RAN downlink control signal, interacting with the strongest cell tower, and then attaching to the cellular RAN. A managed access system "intercepts" contraband cell phones by presenting a stronger RAN presence to a cellular device, overwhelming signals from nearby commercial RAN's. Device to tower communications occurring via the RAN air interface uplink/downlink connections and network core should be further envisioned as providing/having two distinct components: network signaling and customer traffic.



Source: Phil Harris, Engility Corporation

Figure 20. Cellular Radio Access Network

Managed access technology leverages the distinct split between network control and user connection aspects of cellular technology by "managing" network services granted to a specific end user or device. When a cell phone is turned on it initializes its operating system software, searches for and finds a compatible RAN and then connects to the strongest cell tower. Overhead signaling communications processes are used to first "capture" and then direct how the cellular device interacts with the network. This overhead process is used to identify the device, manage how the device interacts with core network resources (i.e., cellular base stations, cell towers, radio frequencies cellular services.)

Signaling transactions between the device and network that pass through the RAN are essentially part of a process used by the network to capture, identify and then verify service levels available to the calling device. Once a device is captured the network can control service provided to the device. Wireless network backbone capacity is typically limited; therefore it is allocated to customers for services on an as-needed basis. The network establishes and then releases network resources as calls, data connection requests, or when inbound received calls are

directed from the network towards/from a specific cellular device. These control communications are often referred to, collectively, as "overhead" communications. Overhead communications associated with network and service management constantly occur and from a resource perspective are typically minimal in comparison to bandwidth required to support user voice or data communications.[33]

Phrased differently, a contraband cellular device essentially "roams" onto a managed access system when it is operated in a managed access RAN coverage area. Once connected to the managed access system RAN, it becomes subject to MAS control[34]. Managed access technology is used to enforce agency policy defining which calls can be completed and which calls are terminated. A managed access system also provides the ability to selectively complete authorized call requests made to/from specific cellular devices, to include emergency calls. MAS operation is guided by facility policies and legal guidelines. In addition to managing the use of contraband cellular devices, managed access systems can be used to capture data about the illegal devices that attach to the system and/or data related to call attempts made from attached devices for investigative purposes.

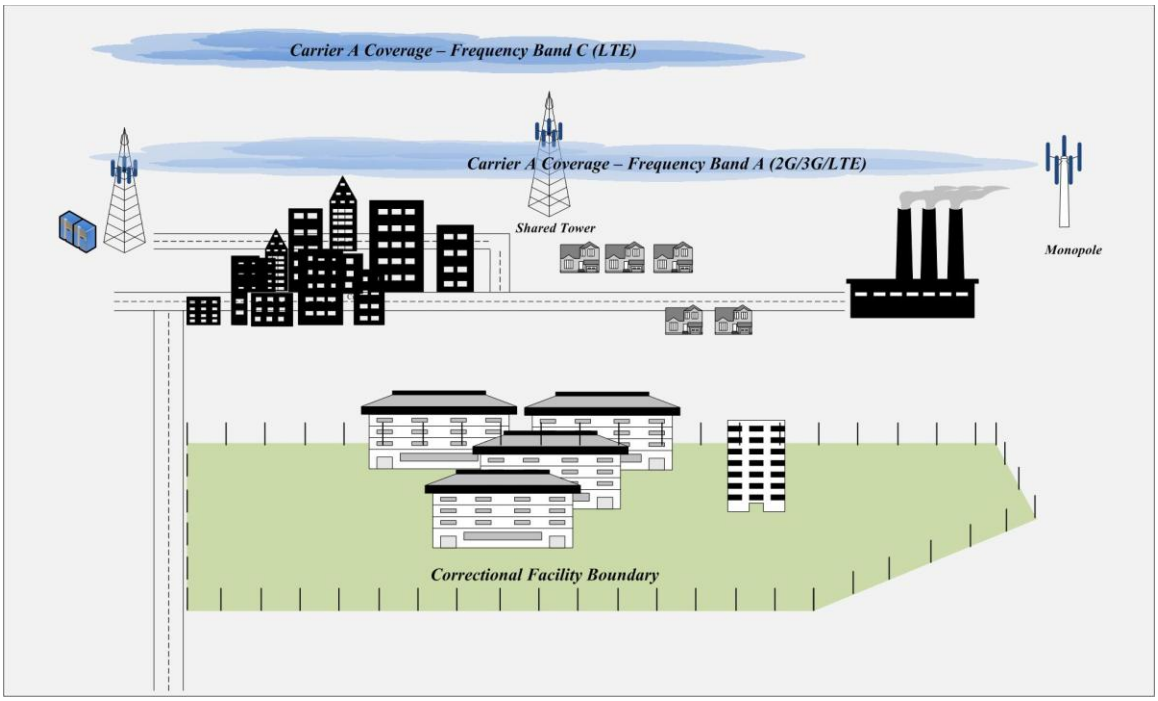
Managed Access Network Coverage

Wireless network signal coverage, envisioned from a simplified conceptual perspective, can be thought of as an invisible cloud of RAN energy that operates at specific radio frequencies. RAN energy within the coverage cloud associated with a network is additive, comprised of

[33] The term Over The Top, or OTT communications described 3rd party services that occur entirely outside of carrier core network resources. OTT communications and OTT overhead are not directly mitigated by managed access, but OTT services are indirectly denied/ blocked when data services are denied by managed access technology.

[34] The term "roaming" is used loosely here; managed access systems actually appear to be part of the commercial network by presenting a valid commercial cellular Mobile Network Code to cellular devices. Outbound service requests are explicitly "denied" or "blocked". Inbound requests are also defeated because the managed access system does not make unauthorized phones visible to the commercial networks; therefore inbound calls to unauthorized phones connected to the managed access network cannot be completed.

overlapping signals emitted from antennas located on adjacent cell towers that operate using the same frequencies. Areas in commercial networks with inadequate signal levels are often described as "coverage holes"[35]. Transmitter components in a portable/mobile cellular device also emit a similar cloud of radio frequency energy, centered on the current location of the device.



Source: Phil Harris, Engility Corp.

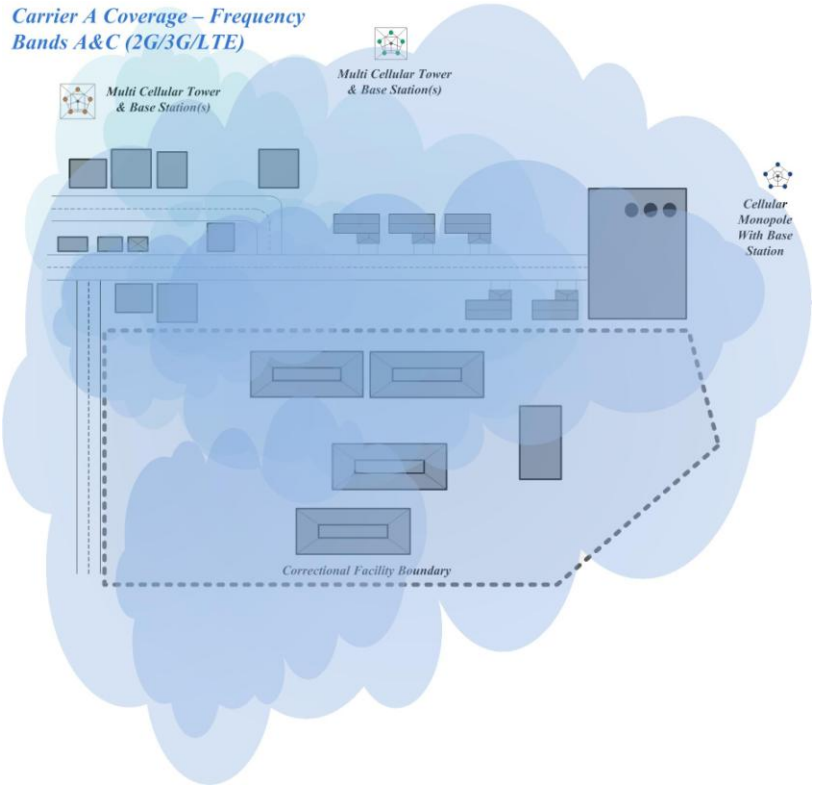
Figure 21. Conceptual View of a Correctional Facility and Nearby Environment

How radio energy propagates through the atmosphere is predictable, with some practical limitations, particularly in highly engineered cellular environments.

Figure 21 depicts a hypothetical correctional facility located adjacent to a town and residential area. At the risk of oversimplification, for the purposes of illustration, RAN signals from competing commercial cellular carriers are depicted using different colors. In this example

[35] Note that the term "coverage hole" in context of commercial network coverage describes an area from which calls cannot be completed. A "coverage hole", in context of a managed access (or jamming) system describes exactly the opposite, an area within the managed access footprint from which connection to a commercial network can be completed. Both describe locations with inadequate signal levels.

"Carrier A" RAN (blue) provides wireless services throughout the town and surrounding areas using two frequencies that including wireless coverage extending throughout the correctional facility. This cellular RAN operates on two different frequency bands (band A and band C, providing differing areas of coverage.) Figure 22 provides a top-down view of the carrier A RAN coverage.

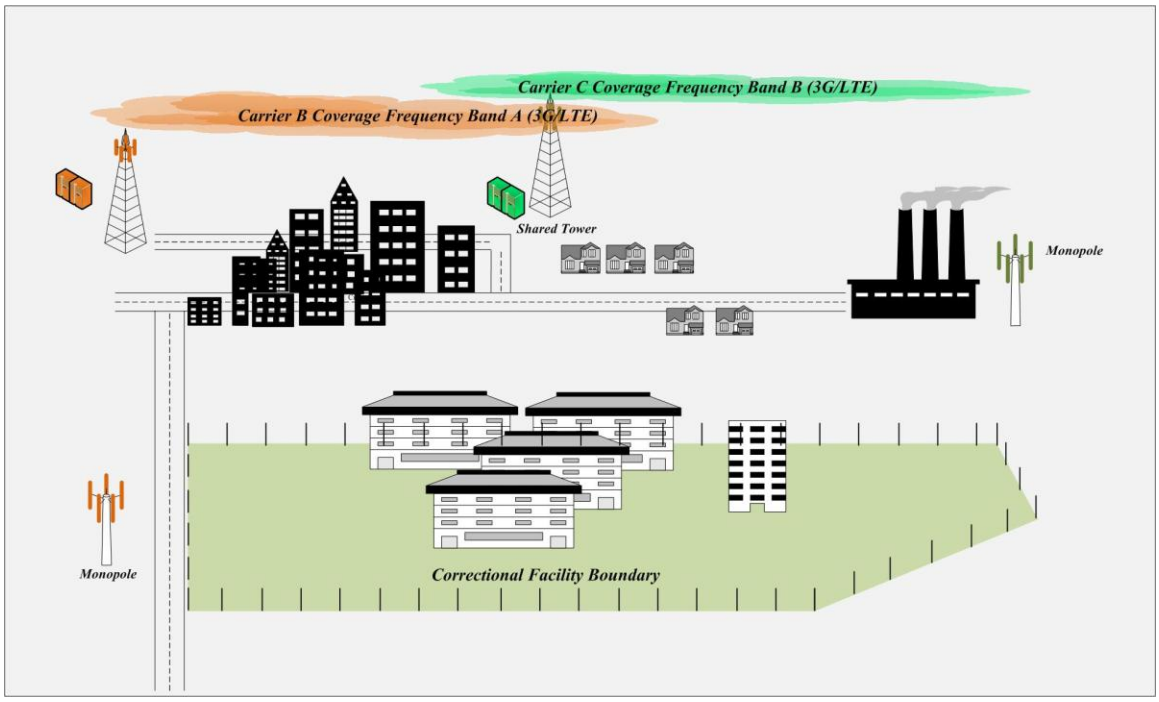


Source: Phil Harris, Engility Corp.

Figure 22. Conceptual Top-Down View of RAN Coverage from Cellular Carrier "A"

To reflect a typical real-world environment two additional, competing RAN networks from carrier B (orange) and carrier C (green) are similarly depicted in Figure 23 and Figure 24. Coverage for each of these three cellular RAN's partially encompasses the hypothetical correctional facility. Each of these RAN's designed and deployed to provide signal coverage tailored to the operator's business model and customer base. Coverage is usually established

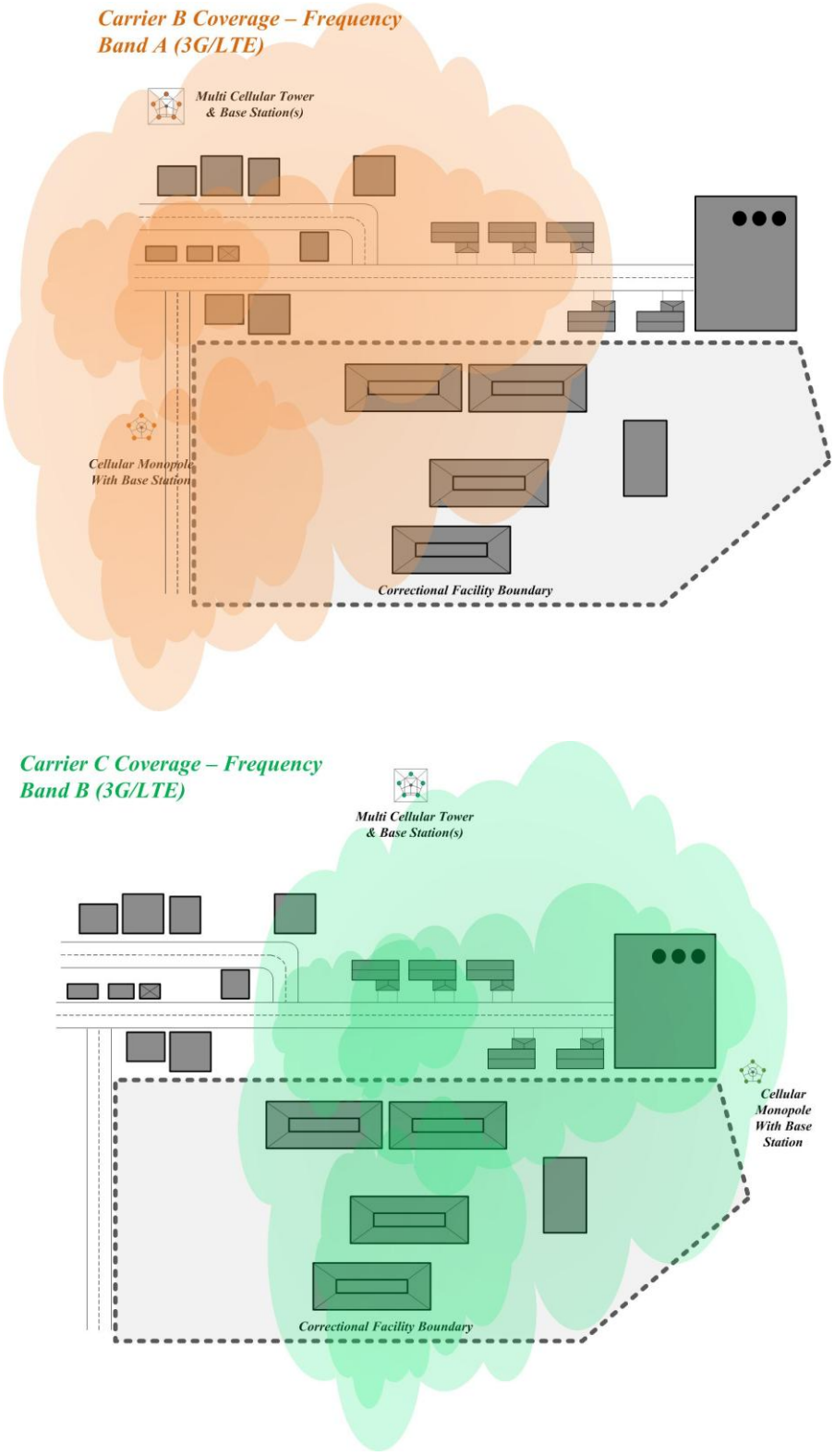
using uplink design criteria associated with a typical portable device performance profile.[36] Some level of inter-carrier resource sharing may occur when common network resources are used, or when a tower is leased to two or more competing carriers. Although each network is unique, there is likely to be significant overlap in overall network coverage.



Source: Phil Harris, Engility Corp.

Figure 23. Conceptual View of a Correctional Facility and Carriers "B" and "C"

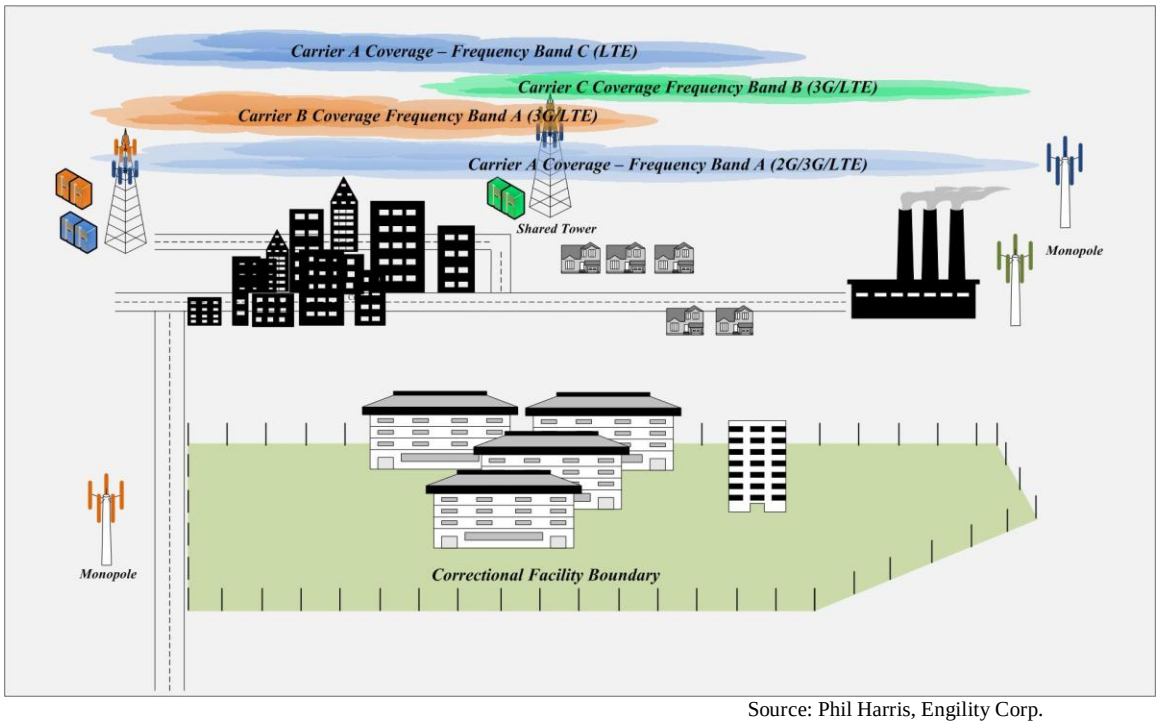
[36] Service performance and wireless range in many environments is typically dependent upon relatively weaker uplink transmissions from a cellular device towards the network, particularly from within buildings and in rural settings where cellular network density results in longer wireless links.



Source: Phil Harris, Engility Corp.

Figure 24. Top-Down View of RAN Coverage from Cellular Carriers "B" and "C"

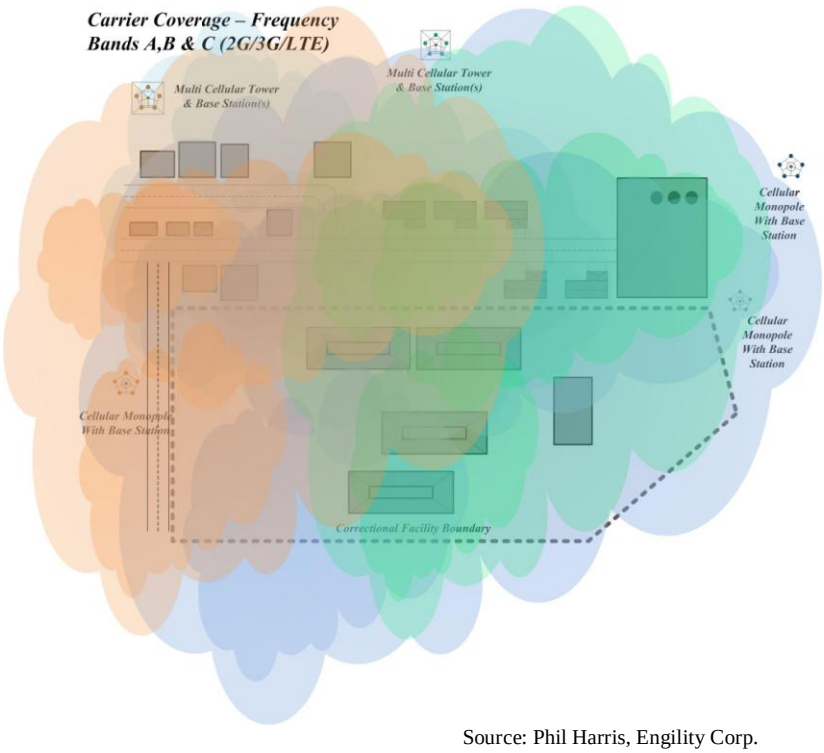
Figure 25 and Figure 26 combine individual carrier views to provide a single view of all three carrier RAN's. They are included to depict the complexity of the entire cellular wireless environment, and how combined cellular carrier RAN coverage overlaps throughout the correctional facility.



Source: Phil Harris, Engility Corp.

Figure 25. Hypothetical Correctional Facility with Carriers "A", "B" and "C"

It is important to acknowledge, and understand this complexity as a combined threat, because any technology deployed to counteract illegal operation of cellular telephones in a correctional environment must, simultaneously, address the entire combined scope to prevent illegal devices from connecting to each carrier network.



Source: Phil Harris, Engility Corp.

Figure 26. Top-Down View: Signal Coverage: Cellular Carriers "A", "B" and "C"

It is also important to note that the commercial carrier network environment is not static. Carriers have the freedom to change the topology and makeup of their network to optimize how RAN interface frequencies and other network resources support their business model. Towers/network base stations, and carrier-specific network protocols are all subject to change as the commercial networks evolve. Commercial RAN's are not fully interoperable and each must be addressed separately because of differences in radio frequencies and protocols. For instance, Carrier A and Carrier B may both operate within the same frequency band, yet customer devices may not be interoperable with both networks because they have licensed and use different sub-allocations within the band. Carrier network changes lead to changes in how cellular customer devices operate, and which uplink/downlink frequencies and/or protocols are used in the RAN to support services. RAN coverage will change over time as well because cellular operators continually optimize their networks. Because of this, technology used to counteract the illegal

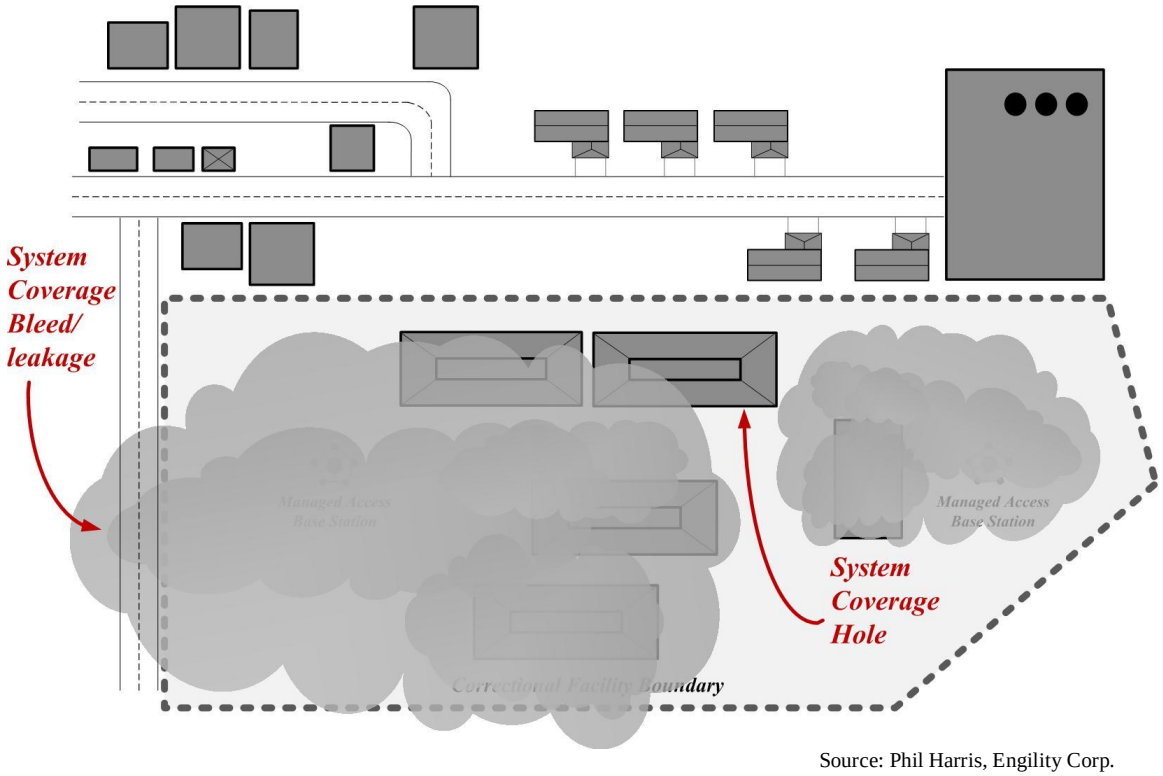
use of cellular devices must also be adapted to ensure ongoing effectiveness. A correctional entity operating a MAS or consuming services provided via a leased MAS must ensure that adaptations to counter carrier network changes are handled in a pro-active manner in response to changes or the system will not retain its effectiveness as the surrounding cellular environment evolves and new end-user devices are introduced. Design, deployment, and operation of a managed access system is not a one-time event, it requires ongoing optimization and capability assessment in response to the surrounding environment.

Network Coverage Related Maintenance

Managed access operational conditions are defined within cellular spectrum leases: coverage must not extend beyond a well-defined service perimeter. System coverage changes can have significant impact on effectiveness if RAN coverage holes are created within a correctional facility. RAN coverage holes can allow users to bypass the managed access system and access commercial networks. Conversely, RAN signal leakage that extends beyond the agreed upon managed access coverage area will lead to disruption of legitimate cellular users in areas where the managed access signal strength overwhelms RAN coverage from a commercial cellular system operator. From a legal perspective compliance with coverage limits defined by a spectrum lease must be addressed first, followed by operational effectiveness within that coverage area. Effectiveness is an internal performance issue, unrelated to spectrum lease conditions.

RAN coverage outside the authorized footprint (a.k.a. leakage/bleed) can lead to FCC enforcement action and/or complaints and public relation issues. Coverage issues must be addressed as part of ongoing system maintenance. As previously noted, RAN coverage changes may occur as a by-product of change within nearby cellular networks, or new capabilities

introduced in commercial networks operated in areas adjacent to the correctional facility. For instance, a new commercial tower installation or a change in commercial network parameters (such as addition of a new band or protocol) can directly affect managed access system coverage[37].



Source: Phil Harris, Engility Corp.

Figure 27. Managed Access System Coverage Hole

Coverage issues may also result from RAN infrastructure damage to either the commercial network or to the managed access system. Coverage issues may result from damage due to inclement weather or from component failure. Any change that affects the relative balance between the strength of managed access and nearby commercial network signal strengths must be resolved.

[37] A managed access system design, to include carrier-specific MAS antenna placement, needs to address and optimize coverage for each carrier's frequencies; especially if the towers are not co-located or there are different deployment scenarios and each carrier transmits at different power levels.