



Signal Inhibitor Solutions

Use of jammers in prisons





The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with over 350 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai, Mobile World Congress Americas and the Mobile 360 Series of conferences.

For more information, please visit the GSMA corporate website at www.gsma.com
Follow the GSMA on Twitter: **Twitter:** @GSMA and @GSMALatam



BlueNote Management Consulting specialises in the telecommunications and media sector, working on strategy, public policy and regulation projects in collaboration with the private sector, official agencies and regional entities.

BlueNote has two offices, in Buenos Aires (Argentina) and Bogotá (Colombia). Its team of consultants has a wide range of qualifications and experience in the telecommunications and media sector, gained in consultancy and public and executive positions. BlueNote operates primarily in Latin America, where its consultants have been involved in technical, regulatory and economic aspects of the sector for more than 15 years.

www.bluenotemc.com

Table of Contents

1. EXECUTIVE SUMMARY	4
2. INTRODUCTIONS	7
3. GENERAL CONCEPTS OF SIGNAL INHIBITORS AND MOBILE NETWORKS	8
3.1. RADIO PROPAGATION BASICS	9
3.2. BASIC PRINCIPLES OF MOBILE NETWORKS	10
3.3. MOBILE SIGNAL INHIBITORS (JAMMERS)	14
3.4. IMPACT OF MOBILE SIGNAL INHIBITORS (JAMMERS)	19
4. INTERNATIONAL EXPERIENCE	22
4.1. OVERVIEW OF MOBILE SIGNAL INHIBITORS (JAMMERS) IN LATIN AMERICA	23
4.2. COMPARATIVE ANALYSIS OF REGULATORY FRAMEWORKS ON THE USE OF JAMMERS	25
4.3. GOOD PRACTICE IDENTIFIED	29
5. ALTERNATIVE TECHNICAL SOLUTIONS	30
5.1. DESCRIPTION OF ALTERNATIVE TECHNIQUES AVAILABLE ON THE MARKET	31
5.2. ANALYSIS OF ALTERNATIVES	34
5.3. CONCLUSIONS AND RECOMMENDATIONS	36
6. REFERENCES	37
ANNEX I. CASE STUDIES	38
ANNEX II. REGULATORY FRAMEWORKS ON THE USE OF JAMMERS	40

1

Executive summary

The use of mobile communication devices smuggled into prisons is one of the main drivers for implementing technical solutions to block, restrict or inhibit mobile communications signals. One of these solutions is the use of mobile signal inhibitors (jammers).

Signal inhibitors or blockers, commonly known as jammers, are radio devices that intentionally transmit signals to affect, block, interfere with or saturate the communications services of mobile users. This includes calls, text messages, GPS positioning signals, data services and Wi-Fi networks.

These devices are governed by commercial communications systems and radio propagation characteristics. Their coverage depends on two factors - 1) its design (e.g. including transmission power and filter quality) and 2) radio propagation factors (the frequency it transmits on environmental obstacles such as buildings, trees and bodies of water, which can reflect or refract signals or cause them to take several paths).

Signal inhibitors (jammers) generate a signal that is intended to interrupt communication between the base station of a communications network and a user's mobile device. This reduces the ratio between the useful or real signal and the interfering signal measured on the device or at the base station. In these conditions, no digital signal recovery mechanism can differentiate between the signals and it is impossible to

establish or maintain stable communication. Jammers treat all communication attempts the same and do not distinguish between different users trying to establish a connection. This means they cannot discriminate between terminals in their coverage area or prevent blocking of emergency numbers.

In other words, regardless of whether communications are authorised or targeted for restriction, blocking will depend on the power level of the signals generated by the base station or the mobile device and the power level of the interfering signal. Given the inherent functionalities of mobile phone networks and the many radio propagation characteristics that affect the definition of a coverage area, there may be points in the area targeted for blocking, where calls can be established or data services can be accessed. Similarly, there may be points beyond the defined area where communications services are blocked.

Blocking mobile frequency bands is not sufficient to prevent covert communications, because other services or technologies can be used, including Wi-Fi, VHF (walkie talkies) and satellite.

The most common impacts of the use of jammers are:




- a. **Communications are blocked beyond the prison grounds**, preventing users from accessing authorised communications services, including emergency calls.
- b. **Communications services are degraded** the area surrounding prisons, resulting in constantly dropped calls, poor quality of communications and slow data services.
- c. Using jammers with poor quality filters and transmitters can generate **harmful emissions outside the operating band**, affecting radio services that operate in other bands.
- d. When jammers operate in multiple frequency bands, they can generate **harmful interfering signals in other bands** and affect all types of services. They may even obstruct the work of police by blocking law enforcement radio communications systems, due to a phenomenon known as intermodulation products ¹.
- e. **Blind spots can occur inside prisons**, where unauthorised communications can still be established.

The Latin American countries surveyed all have similar experiences in respect to addressing unauthorised communications from prisons. Points in common include the background context, the initiatives for solutions and the institutions involved. In the countries studied, unauthorised use of radio devices that intentionally or maliciously interfere with authorised communications is classified as a clandestine, or unlawful use of spectrum. In the United States, the sale, marketing and importing of these devices is restricted by legislation, although exceptions based on public safety or general interest allow their use in confined spaces, such as prisons. In all the cases examined, it is a requirement that communications services beyond the prison grounds must not be affected.

The following table provides a summary of the main regulations passed in Latin America on the use of jammers.

FIGURE 1

Regulations on jammer characteristics and installation procedures

Device regulation	Minimum device characteristics	Devices
 Brazil National Telecommunications Agency (ANATEL) Resolution 306/2002 Resolution 308/2002	<ul style="list-style-type: none"> • Block all frequency bands used in telecommunications services • Must not block other frequency bands or beyond prison grounds • Block signals of any technology • Independent power control in each band • Not within reach of inmates • Comply with electromagnetic field exposure limits 	<ul style="list-style-type: none"> • Notify ANATEL 10 days before switching equipment on • Keep telecommunications operators informed • Submit a technical plan • Conduct impact evaluation at test points
 Colombia ICT Ministry – Ministry of Justice (MINTIC -MinJusticia) Decree 768/2011 Resolution 2774/2013	<ul style="list-style-type: none"> • Comply with electromagnetic field exposure limits 	<ul style="list-style-type: none"> • Applicable only to prisons where there is evidence of offences being committed using communications devices • An application must be sent to ICT Ministry with technical specifications; coverage footprint up to 500 m beyond the prison • Switch off in case of outside impact until remedied • Coordinate with telecommunications operators • Quality indicators do not apply in prisons with jammers
 Mexico General Act on National Public Security System Federal Telecommunications Institute (IFT) Federal Law on Telecommunications Technical Provision IFT-10-2016/IFT-10-2016	<ul style="list-style-type: none"> • Must not extend more than 20 m beyond prisons • Send signals when functionality is interrupted • Control from external locations • Independent adjustable power for each band • No visible controls, to avoid tampering • Block the downlink only • Block downlink only • Must not block 380-399.9MHz band • Comply with electromagnetic field exposure limits 	<ul style="list-style-type: none"> • Install equipment to permanently disable or cancel cellular phone signals in all prisons • Operated by authorities other than those of prisons and at external locations

Source: BNMC

1. Comments made to the NTIA by the industry about the deployment of jammers in prisons (NTIA, 2010)

In the countries studied, national laws and regulations state that under prison regulations and the competences of the institutions involved, responsibility for implementing signal blocking solutions lies with detention centres and prisons. Telecommunications authorities have a role in advising and developing regulations applicable to the sector, while communications service operators have a cooperation and advisory role.

Based on the experience in the countries studied and the product portfolio of some of the leading manufacturers of call restriction solutions, such as Harris,

ShawnTech, CellAntenna and SESP, five basic categories of technology solutions for controlling unauthorised communications from correctional centres can be identified: i) blocking by generating interfering radio signals with some selectivity, ii) capturing communications to control access to commercial networks (Managed Access Systems), iii) techniques that mimic a mobile network cell but do not allow access to services (dummy cells), iv) detection, and v) hybrid solutions combining two or more of these techniques.

The following table provides a comparative analysis of the alternatives available.

FIGURE 2

Comparative analysis of alternatives

				Hybrids		
	Selective jammer	Selective managed access	Selective dummy cell	Detection system	Detection + jammer	Detection + managed access
Blocking effectiveness	<ul style="list-style-type: none"> Scalable to all technologies and bands Risk of blind spots 	<ul style="list-style-type: none"> Does not cover Wi-Fi technology Risk of blind spots 	<ul style="list-style-type: none"> Applicable only to cellular mobile networks Risk of blind spots 	N/A Not intended to block communications	<ul style="list-style-type: none"> Scalable to all technologies and bands Risk of blind spots 	<ul style="list-style-type: none"> Does not cover Wi-Fi technology Risk of blind spots
Impact on authorised communications	<ul style="list-style-type: none"> Risk of harmful interference beyond prison grounds Emergency numbers blocked Risk of impact in other bands 	<ul style="list-style-type: none"> Does not generate interfering signals Risk of "capturing" users beyond prison grounds Does not block emergency numbers 	<ul style="list-style-type: none"> Does not generate interfering signals Risk of blocking users beyond prison grounds 	<ul style="list-style-type: none"> Does not generate interference Risk of reporting on users beyond prison grounds 	<ul style="list-style-type: none"> Risk of interference beyond the prison Low risk of authorised users' calls being blocked 	<ul style="list-style-type: none"> Does not generate interfering signals Risk of "capturing" users beyond the prison Does not block emergency calls
Costs and complexity	<ul style="list-style-type: none"> Depends on prison size Risk of vandalism 	<ul style="list-style-type: none"> High cost. Depends on the area, operators, bands and functionalities 	<ul style="list-style-type: none"> Highly complex coordination. Requires multiple solutions for each operator, band and technology 	<ul style="list-style-type: none"> Depends on the type and complexity Risk of vandalism 	<ul style="list-style-type: none"> Depends on the type and complexity Risk of vandalism 	<ul style="list-style-type: none"> High cost
Support for public safety	<ul style="list-style-type: none"> Provides no information 	<ul style="list-style-type: none"> Information about user identification, type of service and receiver 	<ul style="list-style-type: none"> Information about user identification and location 	<ul style="list-style-type: none"> Provides no information 	<ul style="list-style-type: none"> Information about user identification and location 	<ul style="list-style-type: none"> Information about user identification, receiver service and location

Source: BNMC

The table shows that the technical alternatives available on the market to restrict unauthorised communications from prisons do not perform satisfactorily across the differing factors analysed. Thus, each prison should be studied individually to identify the solution that best meets its needs and priorities. It is also advisable to adopt good practice in the installation of radiocommunication systems suggested by the industry and constantly monitor their impact.

The problem of unauthorised communications from prisons must be addressed across the board. This involves revising security procedures to restrict the entry of communications devices into prisons, blocking or restricting unauthorised communications, detecting and seizing contraband terminals that have entered prisons, and analysing intelligence information to follow up incidents and identify patterns of behaviour to avoid reoccurrence.

2

Introduction

The use of mobile communication devices smuggled into prisons to commit offences such as threats, extortion and scams is one of the main drivers for implementing technical solutions to block, restrict or inhibit mobile communications signals. One of these solutions is the use of mobile signal inhibitors (*jammers*).

Jammers are radio signal transmitters that generate waves in the spectrum bands used for mobile communications. They act as high-power noise that blocks, disrupts or interferes with communications received by or sent to mobile network base stations.

Because jammers do not distinguish between users or types of communication, they affect all communications within their reach. This can significantly affect the quality of communications of commercial users in urban areas near prisons. Users may have problems accessing the service and experience dropped calls.

In this context, the GSMA has commissioned BLUENOTE MANAGEMENT CONSULTING to prepare a report outlining how signal blocking or inhibiting systems function and their impact on authorised mobile services, and identify alternative solutions.

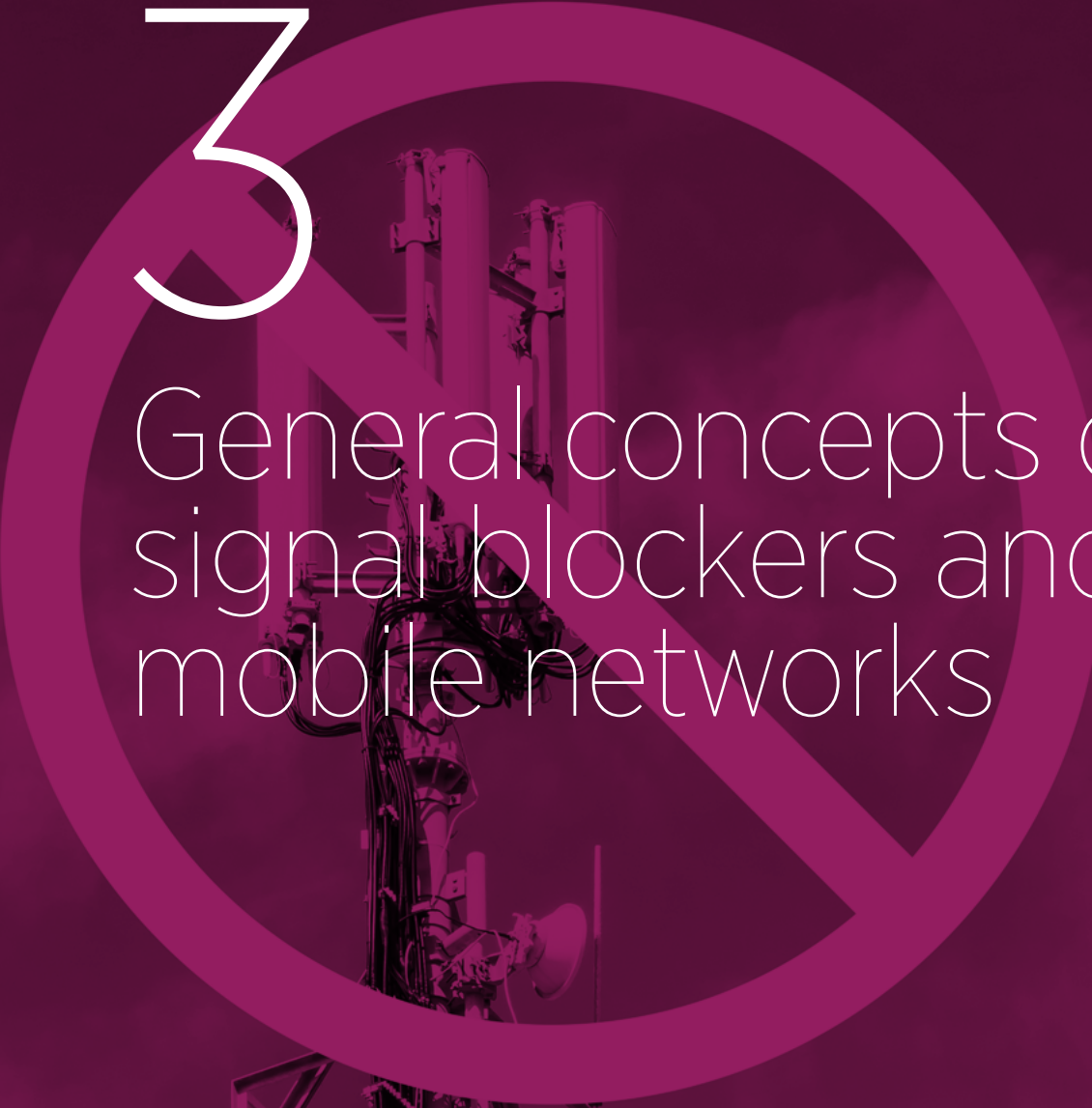
This document is structured as follows:

Chapter 3 briefly explains the principles of electromagnetic wave propagation and how jammers work, including their characteristics, limitations and impact.

Chapter 4 presents the results of a survey of seven Latin American and other countries worldwide about the legal and regulatory framework associated with installing signal blockers in prisons, and identifies good practice.

Chapter 5 describes the alternative technical solutions available on the market to block unauthorised communications in prisons. It includes a comparative analysis of the solutions, conclusions and recommendations of the report.

3



General concepts of
signal blockers and
mobile networks

This chapter outlines the basic principles of radio signal propagation and the functioning of mobile networks and devices that block or inhibit mobile communications. In conclusion, it provides an analysis of how these devices affect communications services.

3.1 Radio propagation basics

Wireless communication services, such as mobile, radio and free-to-air television, are based on the transmission and reception of signals in the form of waves that travel through the radio spectrum to carry information from a transmitting/receiving station to a user's device. For communication to be both possible and satisfactory, each connection must travel in an unused channel - i.e. a part of the spectrum that is not occupied. Because of this, spectrum is divided into frequency bands.

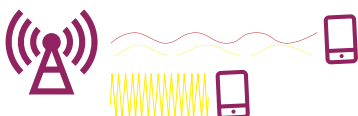
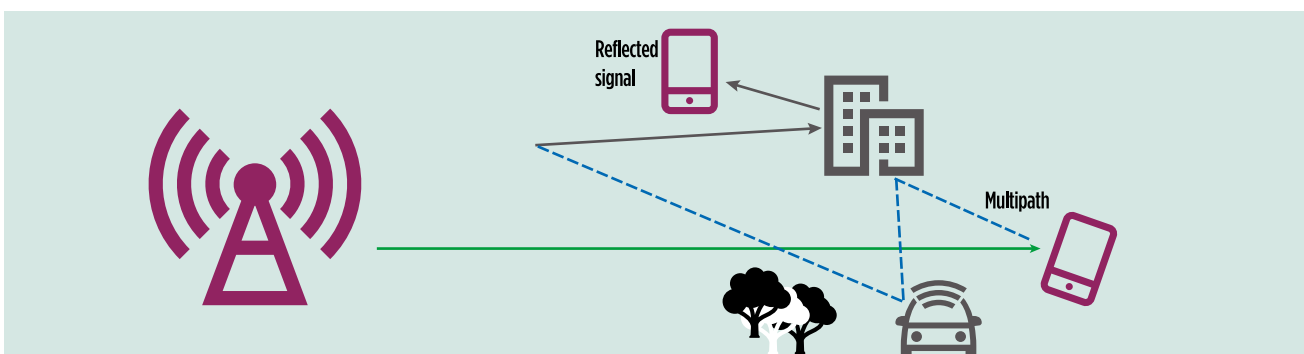
The geographical area where the electromagnetic waves from one or more transmitting stations terminate, or where signals originate, is known as the coverage area.

Coverage depends on factors such as maximum transmitter power and minimum receiver power, operating frequency (low frequencies reach greater distances and penetrate buildings better), quality of the transmitter filter, antenna characteristics (gain to increase the power of the transmitter, ability to focus the signal in a specific direction), and obstacles in the environment, such as buildings, trees and bodies of water, which can reflect or refract signals or cause them to take several paths.

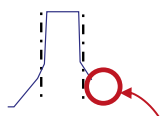
This means that the shape of the coverage footprint of a base station, commonly depicted as a circumference or hexagon, is impossible to predict accurately.

Waves can reach greater distances because of signal obstruction or reflection, e.g., on streets lined with buildings.

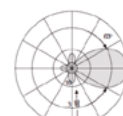
Environmental changes, such as new buildings, different construction materials, new transmitting/receiving stations, temporary faults in the network, technology characteristics or other external factors, can also modify the coverage footprint of a wireless telecommunications network.



Waves are attenuated over distance and are affected by ground conditions, such as buildings and vegetation. Low frequency bands reach greater distances.



Transmitter filters, used to emit signals in only one spectrum range, are imperfect. Emissions are generated outside the band and can affect other services.



Directional antennas cannot focus all signals in one direction, because their materials are not suitable. Emissions occur towards the back and the sides of the antenna.

3.2 Basic principles of mobile networks

Mobile networks are one of the systems that use radio waves to allow communication links for users located anywhere in the network coverage area, even when users are moving. The principle of mobile networks is to divide the coverage area into small cells, thereby allowing spectrum to be reused at different geographical points.

To ensure there are unused channels for each communication established in a mobile network, the technology used for this type of network adopts

techniques to use different time or frequency spaces, or different codes that clearly identify each link. It may also use combinations of these techniques. The evolution of mobile technology from GSM networks to fourth generation

systems - 4G (LTE) - has allowed more efficient use of available spectrum, enabling users to access new and better communications services.

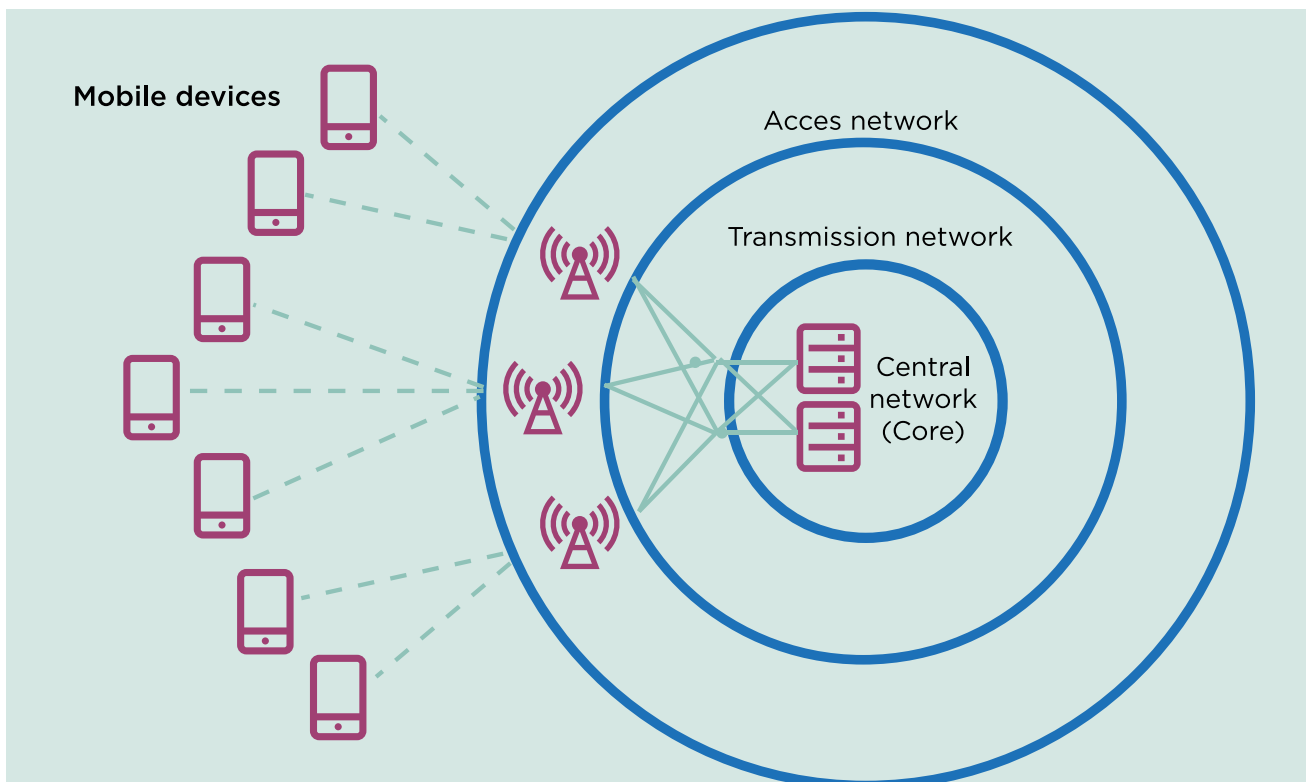
The main objective of any communications network is to ensure user access to communications. As such, mobile networks include signal propagation effects in their designs, adopting techniques to compensate for wave phenomena and ensure the quality of user communications.

Mobile networks typically comprise a series of interconnected systems through which voice and data services can be offered anywhere in the network coverage area via a user's mobile device. Mobile networks have the following basic components:



FIGURE 3

Basic components of a mobile network



Mobile device (terminal)

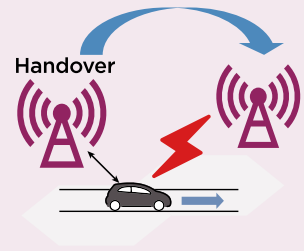
A terminal is the interface between the end user of a mobile network and the operator of a mobile network (radio access network). The terminal must be capable of supporting the technology and the operating band of the network it is attempting to connect to. It contains the identifying information that enables correct registration in the core network. Some terminal models are already equipped with network registration information, but most devices on the market store this information and the operator-defined profile in a removable card, known as a SIM card. Mobile devices can be uniquely identified globally by the IMEI (International Mobile Equipment Identity), a code transmitted by the device when it connects to the network.

Access network

An Access network is a series of transmitting and receiving stations that connect a user's mobile device to the core network - through the transmitting network - to enable communication.

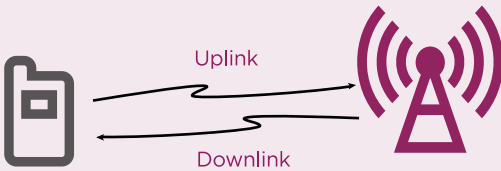
The access network uses the radio spectrum assigned to the network operator to provide the service. Spectrum use requires careful frequency planning to make the best use of available spectrum and avoid interference.

The radio access network transmits messages to a mobile device so it can identify the communications network. It receives information from a mobile device that enables it to request registration in the network or manage a communication link. Alongside other elements of the network, the access network is responsible for maintaining the link so the user remains connected, even when moving, through a process known as handover. This will ensure that a user can switch from one base station to another without losing the communication link.



Communication from the access network to the mobile device is known as the downlink (DL). From the mobile device to the access work, it is known as the uplink (UL).

Most frequency bands currently used in Latin America apply one portion of spectrum for the downlink and another for the uplink. This is known as frequency division duplexing (FDD). There is a mandatory separation between the two portions, e.g., 45 MHz in the 850MHz band. Frequency bands that use the same portion of spectrum for the two links are obliged to use time division duplexing (TDD).



Transmitter network

A transmitter network carries end users' data and voice communications from network nodes (cells) to the central infrastructure of the network (core) and vice versa. It can be implemented using wireless systems (microwaves, satellite, etc.) and/or wire systems (fibre, UTP, coaxial, etc.).

Central network (Core)

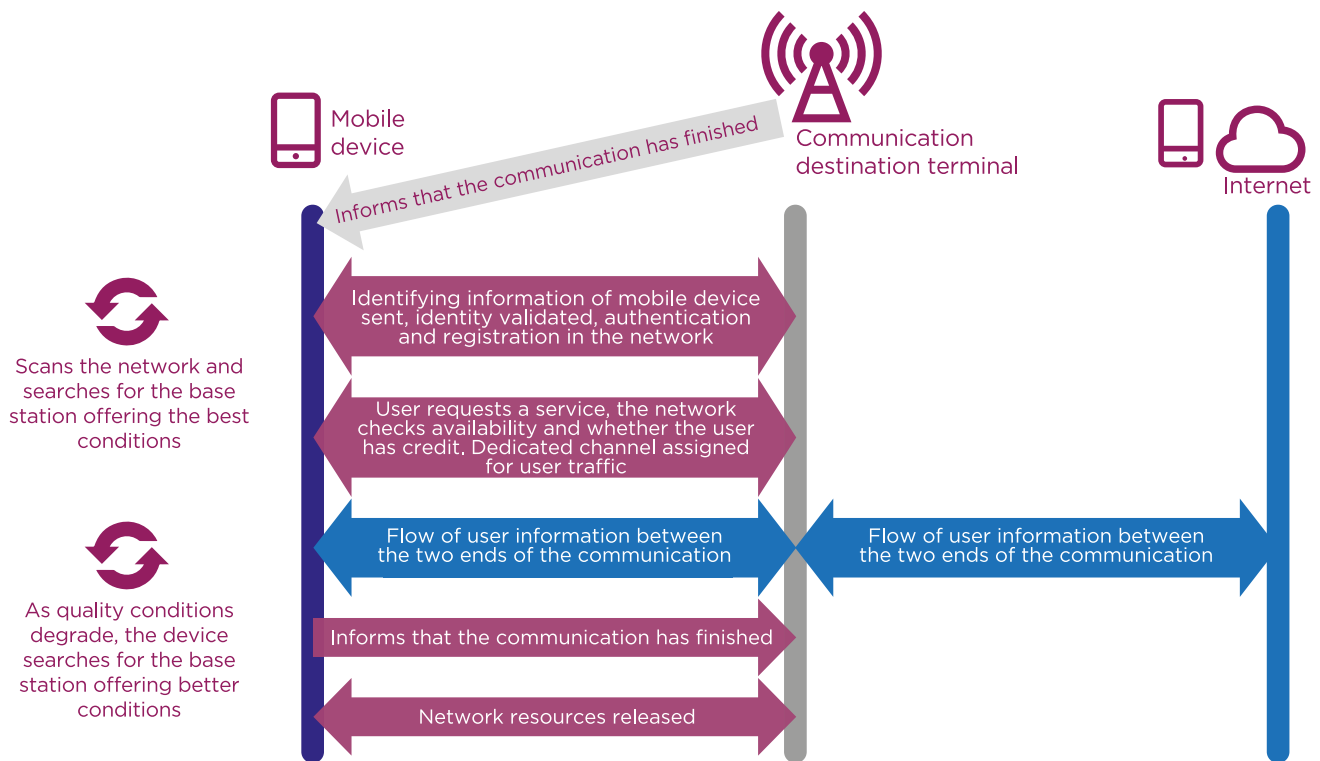
The core is made up of a series of network elements (depending on the technology) responsible for correctly providing the user's service, and the bridges necessary to ensure call switching and data browsing. The main functions of the core are to:

- Store user data and the services activated on the device;
- Manage and administer access to the mobile network;
- Manage device mobility, allowing devices to move seamlessly between network stations;
- Verify and identify a device's IMEI (International Mobile Equipment Identification); this makes it possible to determine the model of the terminal connecting to the network and block stolen devices by the use of EIR (Equipment Identity Register);
- Provide interconnection to other mobile operators and fixed networks; as well as to the internet connection; and
- Process user information so that voice calls and/or data communication can be established.

Other platforms connected to the core network enable user management, pricing, network monitoring and management, and provision of special services.

FIGURE 5

Processes for establishing communication in mobile networks



Source: BNMC

3.2.2 Factors limiting call establishment or access to data services in a mobile network

As previously indicated, the main goal of communications systems and their operators is to provide access for their users to communications services, while maintaining sufficient levels of quality.

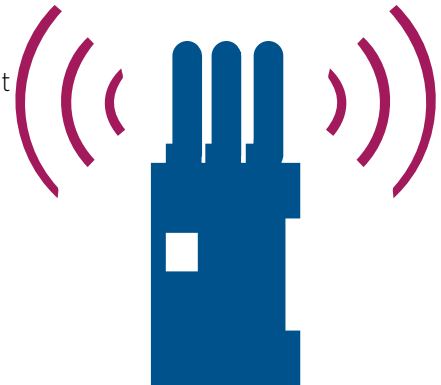
To achieve this, operators apply dedicated engineering to planning, designing and implementing their networks, and constantly monitor them once they are operating. The technology used incorporates functionalities to overcome typical problems that can arise in this type of network, particularly in respect to radio interface due to radio propagation characteristics. These include: frequency hopping techniques to minimise average interference, error correction mechanisms, signalling message retransmission, redundant information sent to compensate packet losses, and monitoring of several base stations from the mobile device to identify which one is best placed to handle communications.

Two types of factors can limit call establishment or access to a data service:

- Non-technical factors include the type of contract with the network operator, billing, user credit, misuse of the mobile device, and use of a blacklisted mobile device with blocked access (e.g., using a stolen terminal).
- Technical factors include: technical faults in any of the components; congestion in network resources (e.g., due to unusual events); and levels of interference above permissible ranges for establishing a service, due to defective filters generating high levels of out-of-band emissions or external interference in the operating band of the mobile network.

3.3 Mobile signal blockers or inhibitors (jammers)

Signal blockers or inhibitors, commonly known as jammers, are devices that disrupt a frequency band to intentionally interfere with electronic equipment attempting to use the radio spectrum. They are most commonly applied to the radio frequency signals of mobile networks, but they can affect any technology that uses their operating bands.



This section provides an introduction to jammers and how they work.

3.3.1 What are jammers and how do they work?

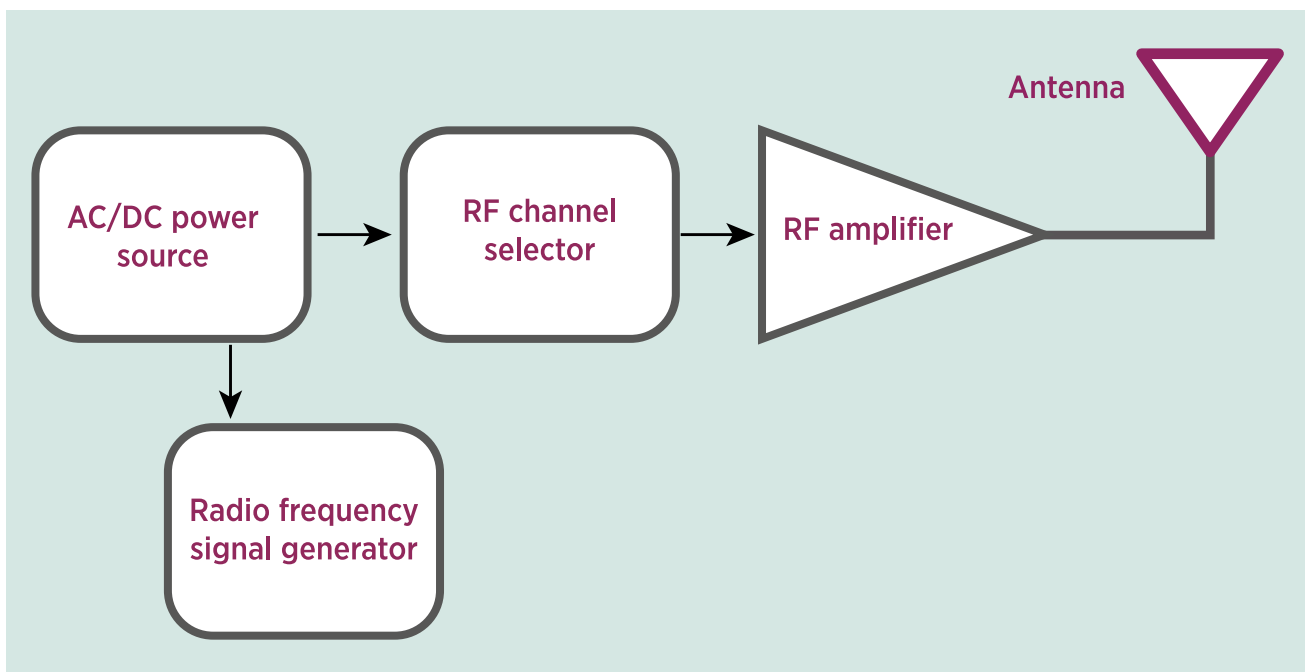
Jammers are radio devices that intentionally transmit signals in specific spectrum bands to affect, block, interfere with or saturate the communications services of mobile users, such as calls, text messages, GPS

positioning signals, data services and Wi-Fi networks. They do this by inserting noise signals or fake information into the frequency. This saturates the band and stops the real information reaching its destination.

3

FIGURE 6

Basic diagram of a jammer



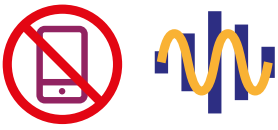
Source: BNMC

Jammers follow basic principles. Their architecture includes an oscillator that generates a signal, a noise generator, a gain phase to give sufficient power to the signal, and one or more antennas. The aim of the signal is to interrupt communication between the base station and the mobile device.

It does this by reducing the ratio between the useful or real signal and the noise or interfering signal so that no digital signal recovery mechanism can establish or maintain stable communication.

FIGURE 7

Principles of operation of signal inhibitors



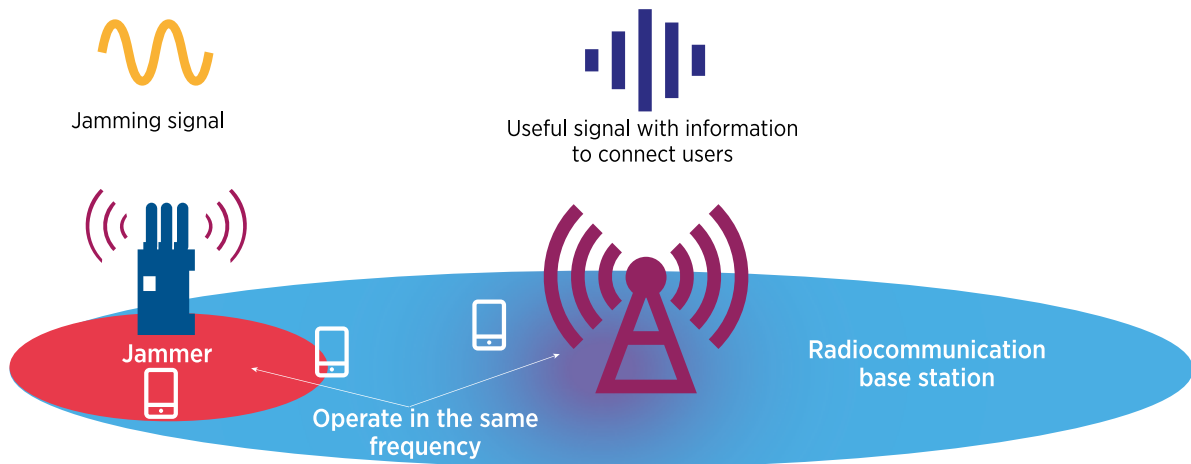
When the jamming signal is the same as or stronger than the signal received or transmitted on the communications network, a block is generated, preventing users from accessing services.



When the jamming signal is lower than but still similar to the communications network signal, a distortion in services is generated, creating a risk of blocking, fault or degradation of quality.



When the communications system signal is significantly stronger than the jamming signals, user messages and information are decoded and communication is possible, with no disruptions.



Source: BNMC

Mobile phones within the coverage area of a base station can normally receive the signals sent by the station. Similarly, a base station can receive all signals generated by radio transmission devices within its coverage area and operating frequency.

When jammers generate an interfering signal in the downlink that competes with the power levels of base station signals, the signal/interference ratio degenerates to such an extent that the signals cannot be decoded. Similarly, when jammers generate an interfering signal in the uplink that competes with the power levels of the mobile device, signals received by the base station (with power levels close to or less than those of the interfering signal) cannot be decoded.

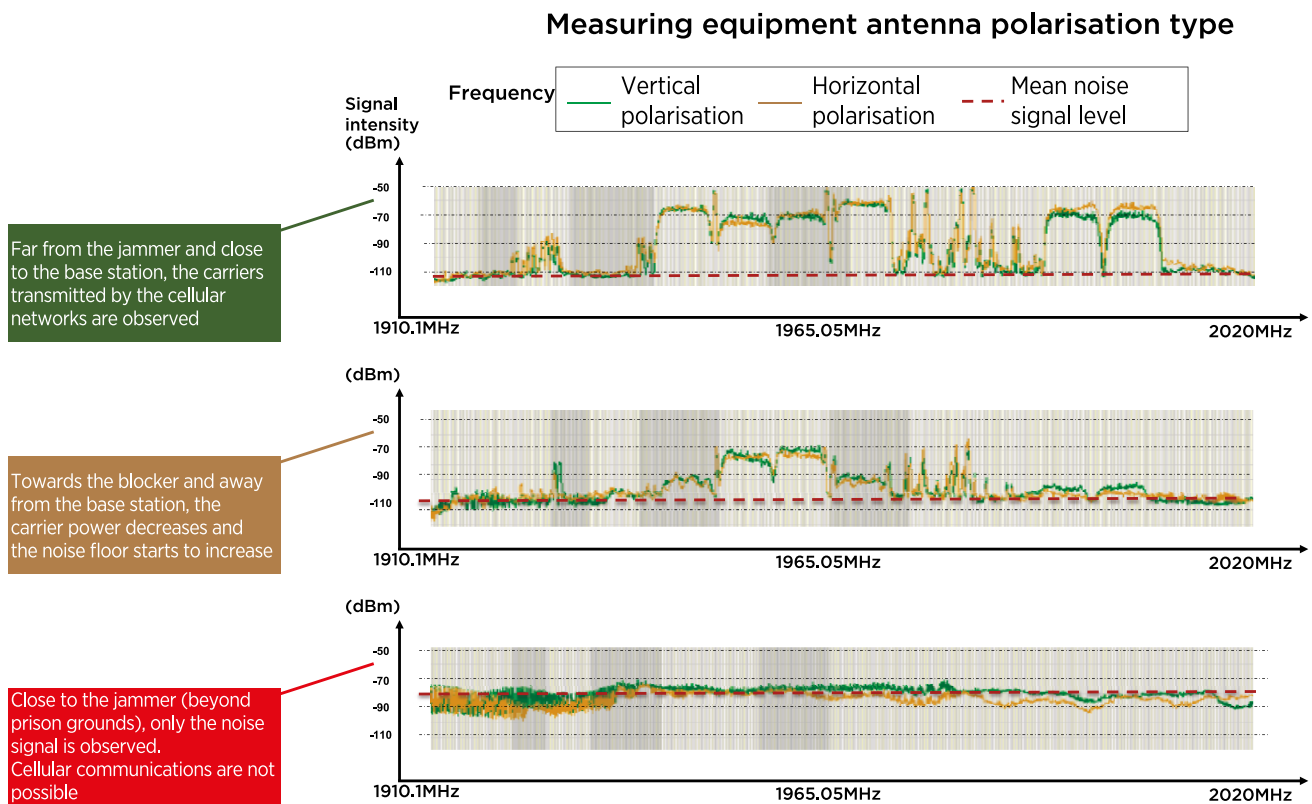
Measurements can be taken to ascertain the effect of jammers on communications services, through tools such as spectrum analysers. These capture all signals transmitted in a specific frequency band. They also observe electromagnetic waves beyond the jammer's area of impact.

In addition to these waves, a noise signal generated by natural factors and easily supported by communications networks commonly occurs in the environment. As the measuring tool is moved further away from the network base stations towards a jammer, the noise signal becomes stronger. The waves carrying the service information deform to the point where they are indecipherable for the systems (mobile device or base station).

These concepts are summarised in the following figure.

FIGURE 8

Real effect of jammers on noise level



3

It is important to note that jammers do not analyse communications attempts or the type of user attempting to establish a connection. This means they cannot discriminate between terminals in their coverage area or prevent blocking of emergency numbers.

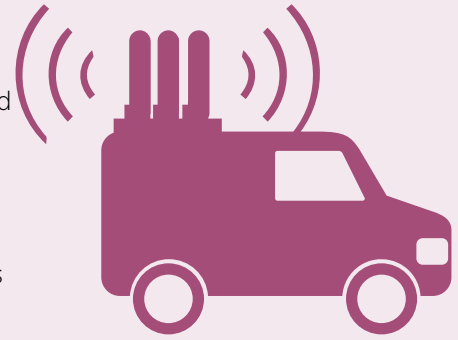
In other words, regardless of whether communications are authorised or targeted for restriction, blocking will depend on the power level of the signals generated by the base station or the mobile device and the power level of the interfering signal. Given the inherent functionalities of mobile phone networks and the many radio propagation phenomena that affect the definition of a coverage area, there may still be points in the area targeted for blocking where calls can be established or data services can be accessed. Similarly, there may be points beyond the defined area where communications services are blocked. Tests conducted in Colombia by the National Penitentiary and Prison Institute found that the effectiveness of blocking communications in prisons can vary from 50% to 99%. Measurements made by mobile operators beyond the grounds of the same prisons showed that access to authorised communications services can be blocked by more than 15%.

Jammers can be classified by their transmitting power, which determines the reach of the device, or by their type of installation (portable, vehicular, fixed, etc.). Each classification includes signal blocking devices or solutions that support one or various frequency bands (usually UHF, mobile and Wi-Fi bands) or use directional or omnidirectional antennas.

Vehicle mounted jammers

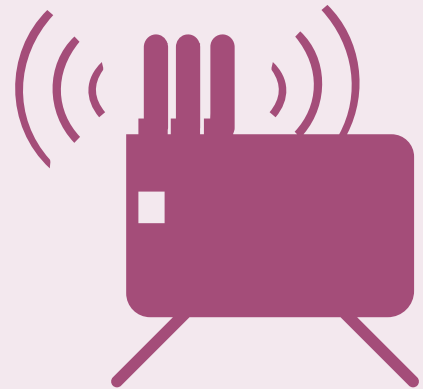
These systems are most commonly used to protect military convoys and vehicles carrying people at high risk of attack from explosives activated by radio detonators (remote control). Signal jammers installed inside vehicles have a range of action of 20 MHz to 3000 MHz and are equipped with high-gain omnidirectional antennas. Their transmitting power is up to 1,600 W and the driver of the vehicle is free to select the frequency channel range in which the interference will take place. Vehicles include an AC generator of up to 10,000 W with a cooling system, ensuring the jamming system is continually available on long journeys. The companies that manufacture this type of jammer offer up to level 6 armouring for vehicles, guaranteeing the protection of the people inside and the blocking equipment.

Some manufacturers of this type of jammer customise the terminal equipment so that the operator or driver can leave radio channels unblocked to allow communication between occupants of the vehicles.



Portable /Tactile jammers

These types of jammers are commonly used by border control agents, hostage negotiators, checkpoint personnel, riot control teams, anti-drug units, bomb squads, SWAT teams, infantry units and many other law enforcement bodies. They are typically housed in wheeled cases or backpacks. Jammers in wheeled cases can have up to 300 W RF output power and simultaneous transmission on three to six frequency bands. Other models can provide jamming on all mobile operating bands and the possibility of blocking up to four bands simultaneously, output power up to 60 W, and an option to include an 8 dBi directional high gain antenna or connection points for 8 dBi to 16 dBi external omnidirectional antennas, depending on client preferences. These types of units operate with internal batteries and AC mains or a DC power source, if requested. For greater mobility, some designs fit inside an attaché case and are more commonly used by personnel patrolling large territories on foot or by bomb disposal squads against remote controlled improvised explosive devices (RCIED). The main features of these type of jammers are that they can block the most commonly used VHF/UHF, satellite and mobile frequencies and are normally equipped with long-lasting rechargeable batteries, ensuring the jammer remains operative for eight hours.



Stationary or fixed jammers

Stationary jamming solutions are designed to provide maximum protection against bomb detonation and undesirable communications in large buildings, establishments and installations such as government prisons, military installations, parliamentary buildings, embassies, detention centres, military shelters, army checkpoints and airports. They can jam RF communication signals in large defined areas.

Their main features include the possibility to provide varying levels of coverage suitable for any fixed-location installation, ability to completely and simultaneously paralyse all communication frequencies from 20 MHz to 3000 MHz without gaps, and up to 1300 W total RF output power. Jamming of each frequency band can be activated or deactivated independently.



The needs of prisons around the world have created a demand for jammers and, therefore, it is common to find devices on the market designed for these types of prisons. The most common features of jammers used in prisons include: i) remote control of the system, giving the operator the option of activating or deactivating each frequency band independently or simultaneously; ii) maximum power output of 100 W per frequency band; and iii) each unit can be equipped with a power adjustment function, enabling the system's RF output power level (coverage radius) to be adjusted according to the requirements of a specific location. Each frequency band has its own high-gain directional antennas (or omnidirectional antennas) with up to 14dBi gain. Antennas can be connected to the jammer units via low-loss cable. They must be connected to AC mains and can be equipped with battery banks in case of mains power failure.

The device ecosystem includes suppliers in various countries, although Israel and the United States have the highest number of market players. Some of the leading manufacturers globally are BAE Systems (UK), Northrop Grumman (USA), Raytheon (USA), HSS Development (USA), Harris Corporation (USA), Lockheed Martin (USA), Israel Aerospace Industries (Israel), PROjammers (HK), Sesp Group (Israel), MCTECH Technology (USA), Wolves fleet Technology Co. Limited (China), PrisonJammer (USA) and SESP (USA).

3



3.3.2 Characteristics of jammers and other solutions

Although there are various types of jammers, they are manufactured with significant differences in their specifications to adapt to different uses or applications. Some of the more important characteristics are:

- Fixed or adjustable output power for each operating band
- Operating frequency bands (DL or UL ranges)
- Out-of-band emissions
- Type of antenna (omnidirectional or directional)
- Remote control and monitoring system
- Power consumption and electrical efficiency
- Portability
- Alarms
- Resistance to environmental factors
- Operating temperature range
- Electromagnetic field levels

Recent developments have enabled jammers to detect the activity of a particular mobile phone and react by blocking its frequencies. Power selectable jammers allow operators to increase or decrease the output level of the jamming signal for stabilised control over the jamming radius. Alternative solutions have been implemented for selective communications blocking. Using radio-based technologies, they detect and block wireless communication devices within their range. These solutions are detailed in chapter 4.

3.4 Impact of jammers

As previously mentioned, the purpose of jammers is to interfere with or disrupt the signals of radiocommunication systems to stop call establishment, texting or access to the internet or data services. Jamming is normally carried out for public interest or safety reasons. However, because of the principles of electromagnetic wave propagation (outlined in section 3.1.), radio transmitting devices can have an undesired impact and affect the communications of commercial users and public safety services, such as emergency numbers.

The greatest impacts of the use of jammers in prisons are:

- a. **Communications are blocked beyond the grounds of prisons**, preventing users from accessing authorised communications services, including emergency numbers.
- b. **Communications services are degraded** in the area surrounding prisons, resulting in constantly dropped calls, poor quality of communications and slow data services.
- c. Using jammers with poor quality filters and transmitters can generate **harmful emissions outside the operating band**, affecting radio services that operate in other bands.

- d. When jammers operate in multiple frequency bands, they can generate **harmful interfering signals in other bands** and affect all types of services. They may even obstruct the work of police by jamming law enforcement radio communications systems, due to a phenomenon known as intermodulation products².
- e. **Blind spots can occur inside prisons**, where unauthorised communications can still be established.

Jamming mobile frequency bands is not sufficient to prevent clandestine communications, because other services or technologies can be used, including Wi-Fi, VHF (walkie talkies) and satellite.

2. Comments made to the NTIA by the industry about the deployment of jammers in prisons (NTIA, 2010)

The following sections analyse these impacts, in particular the jamming and degradation of quality of mobile communications beyond prison grounds. The analysis was conducted using theoretical concepts and measurements made in case studies in prisons in Colombia. These cases are detailed in Annex 1.

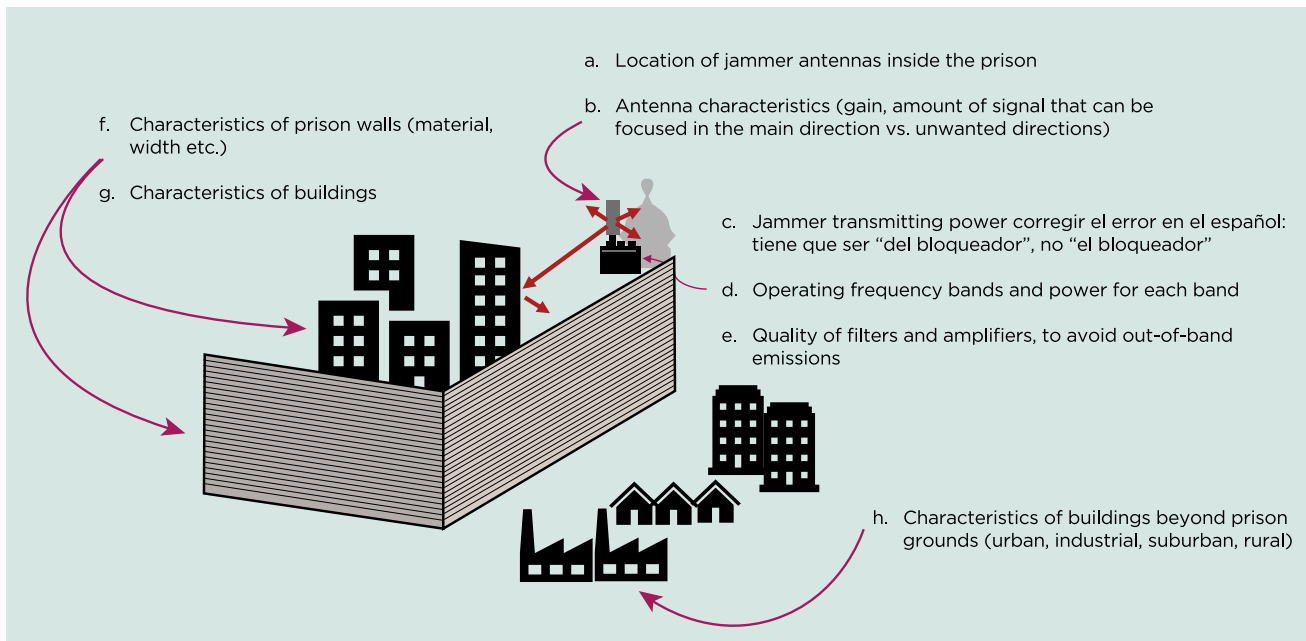
3.4.1 Area potentially affected by the presence of a jammer

As with any radio signal transmitter, the coverage area of a jammer depends on factors associated with the engineering design, the specifications of the equipment installed, and the physical characteristics of the prison and the surrounding area.

The most important of these factors are shown in the following figure.

FIGURE 9

Factors affecting a jammer coverage area



Source: BNMC

The location of the antennas is determined by an engineering study. The aim is to cover the areas targeted for blocking and avoid signal leaks beyond these areas. The study must take into account the physical characteristics of the construction and layout of each prison and the signal levels of the radio communication services targeted for blocking. Antennas located close to the boundaries of a prison or at a height are more likely to cause unwanted interference beyond the prison grounds.

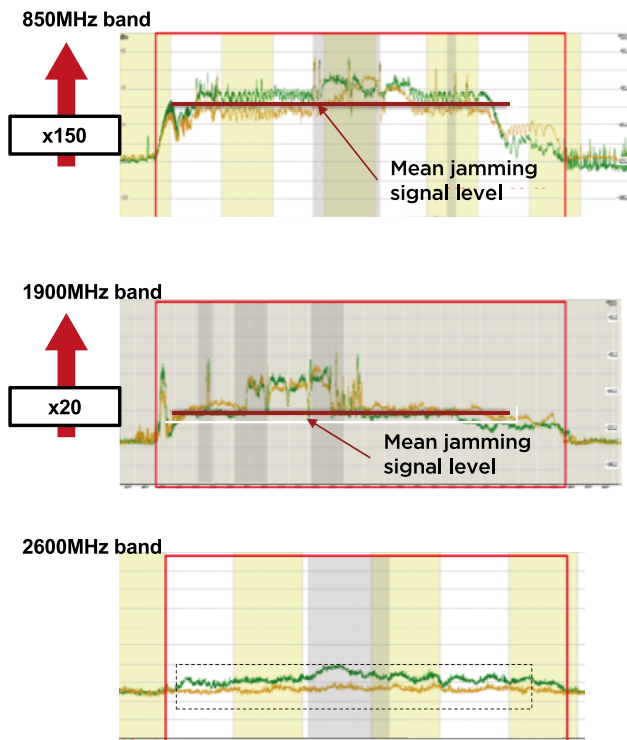
The quality of the equipment and elements installed is another important factor in minimising the risk of unwanted interference. The operating performance of all elements of the system (antennas, connectors, filter and amplifier of the blocking equipment, etc.) has a significant impact on the final result.

The transmitting power generated by the blocking equipment is a key specification to determine the

coverage area for creating interference or restricting communications services. A higher transmitting power results in stronger jamming signals to block communications, but it also has greater impact beyond the prison grounds. High power is normally used to reach areas far from the jammer antennas or improve penetration of blocking signals inside buildings, especially when equipment must be kept out of reach of inmates to prevent tampering or vandalism.

As previously mentioned, signals transmitted in low frequency bands (e.g., 700 MHz, 850 MHz) reach greater distances than signals transmitted on high bands (e.g., 1900 MHz, AWS, 2.6 GHz). Although jammers installed in prisons typically allow independent adjustment of the transmitting power for each operating frequency band, mobile operator tests beyond prison grounds indicated that the interference measured at a given point tends to be much greater in low frequency bands.

For example, in the measurements shown in the figure, the level of the blocking signal transmitted in the 850MHz band is approximately 150 times stronger than in the 1900MHz band.



In the case studies, it was found that the jamming signal runs a critical risk of blocking communications in areas within 400m of prison grounds and significantly degrades the signal/noise ratio in areas 400m to 1,600m beyond the prison. That is, the mean level of the interfering or noise signal increases 10 to 150 times beyond the noise or interference levels normally accepted by radiocommunications systems. However, the studies identified some areas beyond 1,600m where interference levels made it difficult to provide good service conditions.

3.4.2 Impact on user perception

As previously highlighted, users beyond the boundary of a prison can be affected by jammer signals. This is manifested in faults when users attempt to establish communication, dropped calls or session failures during a data connection, or a “No service” message on the phone as it is unable to decode network signals.

With regard to the risk of users being unable to access communications services, the impact measured using information from performance indicators collected by the network and tests carried out beyond prison grounds show a 15% to 60% increase in the probability that users in the affected area will have difficulty accessing mobile network communication services. This means that

because of jammer interference beyond the prison, users will run the risk of blocked communication two to six times out of every 10 attempts. This variation will depend on the user’s location (e.g., distance from the prison) and the traffic demand, which can vary at different times of day.

At base stations that provide coverage to areas near prisons with jammers, the percentage of dropped calls can increase from 2% or 3% to more than 10%, significantly affecting user access.

In technical terms, quality levels of communications services are degraded because the ratio between the network signal and the external interference does not meet conditions for service. It may even reach critical levels where the information transmitted cannot be decoded. The image below shows measurements made by a mobile operator around a prison in Colombia. The red dots indicate points where the degradation in the ratio between the signal and the interference prevents calls being established. The yellow and orange dots indicate points where the ratio has degraded beyond optimum levels to the point where the final quality of the service is affected, but there is still some probability that users will be able to access services.



4

International experience

Smuggling of wireless communication devices into prisons is a worldwide problem, manifested in the significant amount of communications equipment such as mobile phones and SIM cards seized in prisons in countries including Colombia, Brazil, the United States, Mexico, the United Kingdom and New Zealand.

The use of these communication devices by inmates to commit offences such as extortion, threats, kidnapping and murder, or to coordinate escapes, is a priority issue on the public safety agenda of several governments. In recent years, some governments have promoted

coordinated and cooperative efforts among various administrative authorities, and even with the private sector, to identify solutions to tackle this problem. Although progress has been made, regulatory measures adopted have come under serious criticism.

This chapter provides a summary of the situation in some Latin American countries (Mexico, Brazil, Colombia, Argentina and Chile), the United States and the United Kingdom regarding the use of jammers in prisons and the regulatory measures adopted. Further details about each country are included in Annex 1.

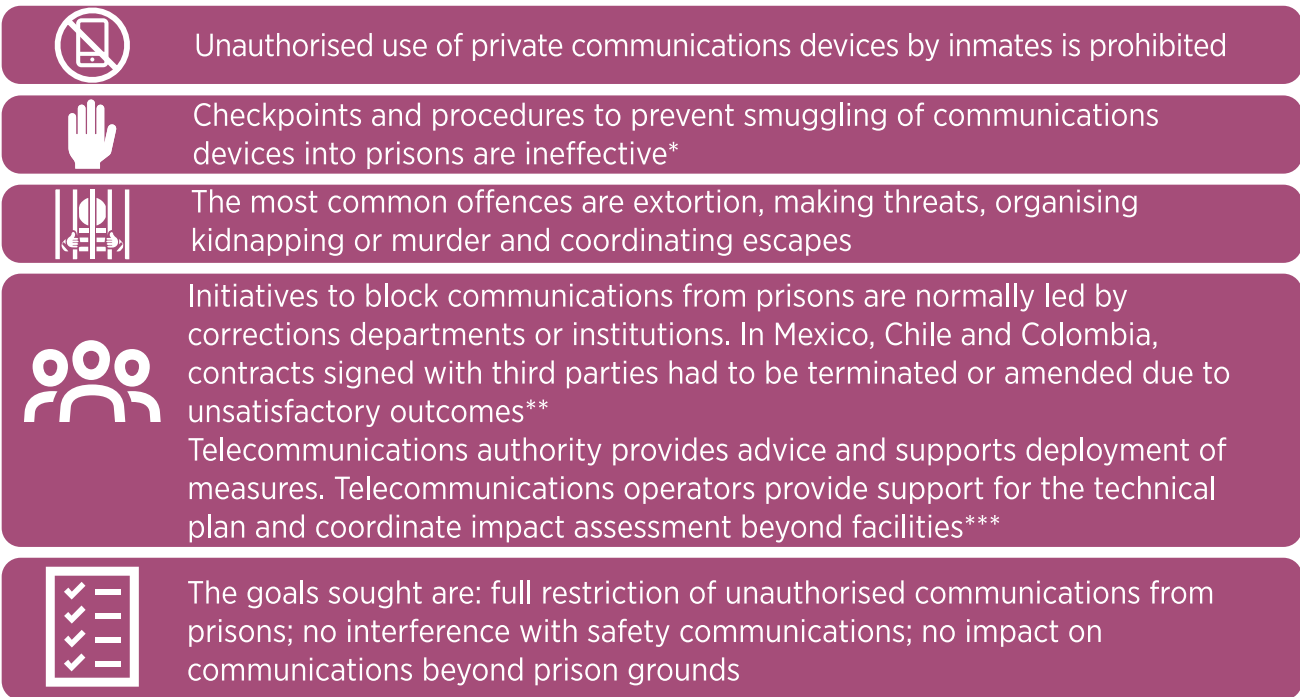
4.1 Overview of jammer use in Latin America

The Latin American countries surveyed have similar experience in the public safety risk of unauthorised communications from prisons and the initiatives used

to combat this problem. Points in common include the background, the solutions and the institutions involved, as summarised in the following figure.

FIGURE 10

Regional overview (background)



* In Colombia there are reports of more than 65,900 terminals seized from 2012 to 2015 . In Chile this figure was 24,992 in 2015⁴.

** A public tender was conducted in Chile in 2012 and a company was contracted to install jammers, but the outcome was unsatisfactory. In Mexico, Software DSI S.A. was contracted in 2011 to install 155 jammers in six prisons.

In Colombia the INPEC has signed various public contracts, one of which was with the company CURACAO.

*** Other public safety agencies such as police intelligence and technological development departments participate as advisors.

Source: BNMC

The communications systems used by inmates include mobile communication terminals, trunking radios, UHF radios, satellite phones, Wi-Fi, GPS and even drones for trafficking in weapons, drugs and communications devices. Despite this, security agencies in the countries surveyed focus on the most commonly used methods, communications through mobile networks and Wi-Fi.

In the countries surveyed and in the United States and the United Kingdom, it is the responsibility of national or local corrections departments or prisons to manage projects and budgets for solutions to block or restrict communications from inside prisons.

In Colombia, the National Penitentiary and Prison Institute (INPEC) managed the installation of jammers in 16 prisons from 2013 to 2016. The prisons chosen had been identified as those with the highest risk of offending, in a work plan that included meetings with the ICT Ministry and mobile operators. Tests conducted by the INPEC showed that the effectiveness of these solutions in blocking calls ranged from 50% to 99% and often inmates had vandalised jamming equipment, causing serious damage.

Using tactical jammers, the INPEC conducted tests in coordination with the National Police Anti-kidnapping and Anti-extortion Directorate. The jammers identified SIM numbers (IMSI) and mobile device codes (IMEI) that could then be blocked by mobile operators⁶.

3. (INPEC, 2016).

4. (Economía y Negocios, 2016).

5. With a rise in drone-assisted smuggling of drugs, weapons and mobile phones detected in prisons in the United Kingdom, signal jammers are being considered as a possible preventive measure.

6. (INPEC, 2016)

Brazil's National Prison Department (DEPEN) has installed blocking systems in 23 prisons in São Paulo, corresponding to 14% of all corrections prisons in the area. Despite this measure, mobile terminals are still being seized in prisons equipped with a jamming system, indicating that the solution is not 100% effective. A few years ago, a proposal was made to oblige operators of telecommunications services to install and operate jamming systems. However, given that public safety is a state duty, with procedures and responsibilities laid down in Brazil's Criminal Enforcement Law, the Federal Supreme Court ruled on 3 August 2016 that this proposal was unconstitutional.

In Mexico, agencies within the Undersecretariat of the National Prison System have been updating regulations and reviewing technical solutions to install jammers in every prison in the country. In 2011, the government of Mexico awarded a contract for installation of jammers in six prisons. The results were poor, due to the low effectiveness of the system and the impact on the mobile service of the neighbouring population. Security agencies reported that the prison population had tampered with the jamming equipment and modified it.

Chile's National prison service, the Gendarmerie, had a similar experience with a contract to install jammers awarded in 2012. Given the limited effectiveness of the jamming system and the impact on civilian communications beyond prison grounds, the Gendarmerie requested information from the industry about solutions to block wireless communication signals inside prisons, with a view to launching another public tender.

In Argentina, a jammer installed in Piñero prison, in the Province of Santa Fe, had a significant impact on the mobile communications services of the nearby population. The National Communications Agency (ENACOM) ordered the jammer to be switched off.

In the United States, which has a strict regulatory framework for use of jammers, some prisons (around 52 in 17 states) have deployed radio-based technologies to detect and block wireless devices inside their boundaries. Known as Contraband Interdiction Systems (CIS), these technologies must be authorised by the FCC. They comprise Managed Access Systems (MAS) and systems that detect devices through user ID (IMSI/IMEI), facilitating the inclusion of user details in blacklists. The United Kingdom has adopted similar measures.

In all the countries surveyed that have deployed jammers, the following undesired effects were observed:

- It was not possible to reach or ensure 100% efficiency in blocking unauthorised communications from prisons.
- The communications services of the population beyond prison grounds were degraded, affecting user access to authorised communications networks.
- Inmates vandalised and tampered with jamming equipment.

7. Estimates indicate an investment of 31 million Reales. (GLOBO - EPOCA NEGOCIOS, 2017)

4.2 Comparative analysis of regulatory frameworks on the use of jammers

The regulatory framework applicable to the use of jammers can be examined from two angles, considering jammers as: i) devices that emit radio signals and use radio spectrum, and ii) security devices for delinquency and crime prevention.

The following sections summarise the main aspects of current legislation in the countries surveyed with regard to the abovementioned approaches.

4.2.1 Regulations applicable to devices that emit radio signals and use radio spectrum







Unauthorised use of radio frequency devices that intentionally or maliciously interfere with authorised communications services is prohibited in the countries surveyed, or considered clandestine or illegal use of spectrum. However, certain exceptions, on the grounds of public safety or general interest, allow deployment of jammers in confined spaces, such as prisons.

All the cases examined stipulate that authorised communications services beyond prison grounds must not be affected.

The following figure provides a summary of key aspects regarding regulations.

FIGURE 11

Regulations applicable to jammers as spectrum-using devices

Equipment regulations	Use of jammers	Exceptions
 Argentina National Communications Agency (ENACOM) Argentine Digital Law	<ul style="list-style-type: none"> Interfering with authorised communications services is illegal use of spectrum 	<ul style="list-style-type: none"> N/A
 Brazil National Telecommunications Agency (ANATEL) Resolution 308/2002	<ul style="list-style-type: none"> Interfering with or restricting authorised signals is clandestine use of spectrum 	<ul style="list-style-type: none"> Use of radiocommunication signal jammers authorised in prisons. MUST NOT AFFECT SERVICE BEYOND PRISON GROUNDS
 Colombia ICT Ministry - National Spectrum Agency (MINTIC - ANE) Resolution 2774/2013	<ul style="list-style-type: none"> Using jammers is clandestine use of spectrum 	<ul style="list-style-type: none"> Public entities or financial sector, for public safety or general interest, with authorisation from ICT Ministry. Switch off when outside areas are affected State security agencies may use jammers without authorisation
 Mexico Federal Telecommunications Institute (IFT) Federal Law on Telecommunications	<ul style="list-style-type: none"> Disabling or cancelling radiocommunication signals is legal only in prisons 	<ul style="list-style-type: none"> Mandatory use in all social reintegration and prisons Effects must not extend more than 20 m beyond prison grounds
 United State Federal Law on Telecommunications (FCC) Telecommunications Act	<ul style="list-style-type: none"> Use, sale, importation and marketing of jammers prohibited 	<ul style="list-style-type: none"> Manufacture for export only Used by US government with FCC authorisation
 United Kingdom Office of Communications (Ofcom) Section 68 Wireless Telegraphy Act 2006	<ul style="list-style-type: none"> Installing wireless devices is prohibited in UK mainland, Northern Ireland and territorial waters, the Isle of Man and the Channel Islands 	<ul style="list-style-type: none"> Confined precincts inside prisons. Must not affect outside areas



4.2.2 Regulations applicable to devices deployed to prevent delinquency and crime




As mentioned in the previous section, spectrum regulations allow certain exceptions for the use of jammers. In some cases, additional regulations have been issued that define aspects such as the

specifications of the authorised equipment, the roles of the parties involved, and authorisation and monitoring procedures.

The following figure summarises some of the regulations related to jammers.

FIGURE 12

Regulations on jammer specifications and procedures

Device regulation	Minimum device characteristics	Devices
 Brazil National Telecommunications Agency (ANATEL) Resolution 306/2002 Resolution 308/2002	<ul style="list-style-type: none"> Block all frequency bands used in telecommunications services Must not block other frequency bands or beyond prison grounds Block signals of any technology Independent power control in each band Not within reach of inmates Comply with electromagnetic field exposure limits 	<ul style="list-style-type: none"> Notify ANATEL 10 days before switching equipment on Keep telecommunications operators informed Submit a technical plan Conduct impact evaluation at test points
 Colombia MICT Ministry – Ministry of Justice (MINTIC -MinJusticia) Decree 768/2011 Resolution 2774/2013	<ul style="list-style-type: none"> Comply with electromagnetic field exposure limits 	<ul style="list-style-type: none"> Applicable only to prisons where there is evidence of offences being committed using communications devices An application must be sent to ICT Ministry with technical specifications; coverage footprint up to 500 m beyond the prison Switch off in case of outside impact until remedied Coordinate with telecommunications operators Quality indicators do not apply in prisons with jammers
 Mexico General Act on National Public Security System Federal Telecommunications Institute (IFT) Federal Law on Telecommunications Technical Provision IFT-10-2016/IFT-10-2016	<ul style="list-style-type: none"> Must not extend more than 20 m beyond prisons Send signals when functionality is interrupted Control from external locations Independent adjustable power for each band No visible controls, to avoid tampering Block the downlink only Block downlink only Must not block 380-399.9MHz band Comply with electromagnetic field exposure limits 	<ul style="list-style-type: none"> Install equipment to permanently disable or cancel cellular phone signals in all prisons Operated by authorities other than those of prisons and at external locations




Source: BNMC



The following figure shows the responsibilities of each party involved in deploying and/or operating jammers

FIGURE 13

Responsibilities of parties involved in deploying or operating jammers

Telecommunications operators	Telecommunications authority	Department/agency/prison
 Brazil <ul style="list-style-type: none"> Confidentiality of information Report changes in the network that affect coverage in areas of interest Collaborate with impact evaluation at test points 	<ul style="list-style-type: none"> Block all frequency bands used in telecommunications services Must not block other frequency bands or beyond prison grounds Block signals in any technology Independent power control in every band Not within reach of inmates Comply with electromagnetic field exposure limits 	<ul style="list-style-type: none"> Notify ANATEL 10 days before switching equipment on Keep telecommunications operators informed Submit a technical plan Conduct impact evaluation at test points Manage budget and contracts; install and operate system
 Colombia <ul style="list-style-type: none"> Collaborate with authorities Restrict transmitting, receiving or control signals inside prisons when required by ICT Ministry 	<ul style="list-style-type: none"> Check effects on areas in the vicinity of prisons Analyse and authorise applications to use jammers Provide advisory services to prisons 	<ul style="list-style-type: none"> Applicable only to prisons where there is evidence of offences being committed using communications devices An application must be sent to the ICT Ministry with technical specifications; coverage footprint up to 500 m beyond the prison Switch off in case of impact beyond prison until solved Coordinate with telecommunications operators Quality indicators do not apply in prisons with jammers Manage budget; install and operate system
 Mexico <ul style="list-style-type: none"> Collaborate with authorities on technical matters to disable or cancel cellular telephone signals in prisons Collaborate to monitor operability of jamming equipment 	<ul style="list-style-type: none"> Support and advise corrections and safety authorities Coordinate with telecommunications operators Monitor quality of service in surrounding area 	<ul style="list-style-type: none"> Coordination among entities Administer budget and tendering Install, operate and supervise function

Source: BNMC



4.3 Good practice

The experience in the countries surveyed reveals good practice in encouraging compliance with the government objectives shown in Figure 12.

Review the protocols and procedures to control the entry of communications devices into prisons and strengthen detection tools

Communications for unlawful purposes start with the smuggling of mobile phones and other communications devices into prisons. Smuggling can be achieved through inadequate procedures at points of entry for outside personnel, assistance from prison guard staff, or other methods.

To address this aspect, the work plan of Colombia's National Penitentiary and Prison Institute (INPEC) included an initiative to review the protocols and security procedures for the entry of items into prisons⁸.

With the support of the National Police, the INPEC has conducted tests using tactical equipment to detect radiocommunications devices inside prisons. Once devices have been detected, they can be seized or the user's identifying information can be blocked. This type of equipment is already in use in the United States and the United Kingdom.

Identify prisons that clearly require a mobile communications blocking solution

Deploying signal blocking devices in prisons across a country significantly increases the probability that the general public and public authorities will be unable to access communications services, especially in emergencies. Installing and effectively operating this solution is also a considerable expense for public entities.

Colombia has focused solely on prisons where there is evidence of offences being committed from inside the prison using communications devices. In some cases, offenders have been relocated so they can be grouped in prisons where signal blocking is authorised. In Brazil and the United States, prisons intending to deploy this solution must submit an application and obtain authorisation to use signal blockers.

For relocation of inmates linked to offences of extortion, kidnapping etc. committed from prisons, priority should be given to prisons in rural areas or locations away from populated areas that could be affected by the solution.

Analyse and define the technical solution for each prison according to the needs and characteristics of each case

The prisons in a country can differ in their location (urban or rural), type of construction (characteristics of walls and buildings), internal layout and network operator coverage levels. They can also have different needs and requirements, such as the type of communications devices used and the risk level. It is important to analyse the appropriate solution for each prison (a single technology or a combination of strategies) to obtain a better cost impact/benefit ratio. Reports by the FCC, in the United States, support this strategy.

The same solution should not be applied across the board in all prisons based on the positive results of just one test case.

Coordinate with authorities from the ICT sector and telecommunications operators for information flow and collaboration. Conduct controlled tests

8. (INPEC, 2012)

Collaboration between prison authorities, ICT sector authorities and telecommunications service operators is common in Colombia, Mexico, Brazil, the United States and the United Kingdom. Using this strategy, the parties involved can identify alternative solutions, mitigate or at least monitor the impact in areas beyond prison grounds, and where necessary, implement regulations and procedures.

Recognise the risk of blocking access to communications for users beyond prison grounds and define clear procedures for action

Regulations clearly prohibit any impact on communications services beyond prison grounds. In Colombia, regulations require the signal blocker to be switched off immediately when the neighbouring area is affected until the problem is solved and the corresponding tests and measurements have been conducted. It is also a condition that mobile operators should not be penalised for any degradation of service caused by interference from signal blocking devices.

Continually review the state of the art of technologies that block and/or restrict unauthorised communications from prisons

Another common practice is to request up-to-date information from manufacturers and the industry about solutions to block or restrict unauthorised communications from prisons. For example, Chile, has issued requests for information in recent years before launching invitations to tender.

Other practices from a technical point of view include:

- Requiring signal blocking equipment to comply with electromagnetic field exposure limits; and
- Restricting jamming signals to the downlink frequency, as laid down in Mexico's regulations. This minimises the risk of interference with mobile networks, but can reduce the effectiveness of the system.



5

Alternative technical solutions

Unlawful use of communications devices from prisons to commit crimes is a reality that affects public safety and requires authorities and governments to take pre-emptive measures. However, it has been established that using technological solutions that generate radio signals to interfere with commercial networks, without determining the identity or the location of the user making or receiving the call, significantly affects the population in the area surrounding prisons. The effects can include limiting or restricting access to authorised public communications services, preventing

communication with emergency services, and disrupting communications intended to protect the public.

The following analysis of the technical solutions available on the market to prevent unauthorised communications in prisons can also be applied to assess alternatives for regions such as Latin America.

5.1 Description of alternative techniques available on the market

The experience of the countries surveyed and the product portfolio of some of the leading manufacturers of call restriction solutions, such as Harris, ShawnTech, CellAntenna and SESP, focus on five basic categories of technological solutions that control unauthorised communications from prisons. These are based on: i) blocking with some level of selectivity by generating interfering radio frequency signals, ii) capturing communications to control access to commercial networks (Managed Access Systems), iii) techniques that emulate a mobile network cell, but do not allow access to services (dummy cells), iv) detection, and v) hybrid solutions integrating two or more of these techniques.

The main features of each category are detailed below.

5.1.1 Mobile signal blocking or inhibiting devices (jammers) based on radio frequency signal generation

This category comprises solutions based on the basic principles of the signal blockers or inhibitors described earlier, incorporating analysis techniques to provide some blocking selectivity that reduces the effective interference generated in the system beyond prison grounds.

Some devices scan RF signal activity inside prisons and then block (by generating an interfering signal) only in the range of frequencies⁹ and/or in the geographical area of the activity detected¹⁰.

They also include features such as the use of distributed directional antennas, centralised and remote control (to reduce the risk of vandalism), adjustable power control for each frequency band, blocking of all communications systems operating in the bands carried by the system, and easy scalability to add new frequencies for blocking.

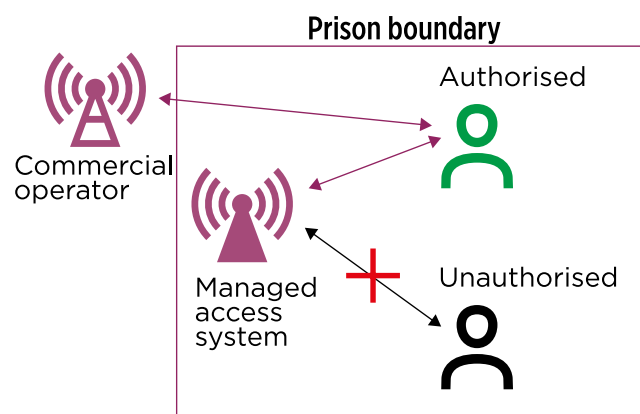
As with traditional signal blockers, implementing this type of solution requires an engineering study to limit the coverage area, as far as possible, to the confines of the prison. Ongoing monitoring of the quality of communications services beyond prison grounds is also necessary. This is because selective blocking techniques

can help to reduce the mean interference generated in the system, however a risk still remains that authorised communications services beyond the grounds of a prison will be affected.

These solutions do not analyse the identity of the user making or receiving the call, or the information transmitted. They provide no relevant information to assist the intelligence work of public safety agencies and there is a critical risk that emergency numbers will be blocked.

5.1.2 Blocking unauthorised communications using managed access

These types of solutions, known as Managed Access Systems, are based on a micro-cellular, private network operating in authorised frequency bands of radiocommunications services. They are an extension of commercial networks, with coverage inside the prison, and include a database to determine which users are authorised to access commercial telecommunications networks (white list).



9. PKI-Electronic PKI-6170 and PKI-6200 jammers detect signal activity and block it in the specific range where it is detected (PKI-ELECTRONICS, 2017).

10. Bahia 21 Corporation made a proposal to develop a spatial analysis technique to block service solely to communications terminals inside an unauthorised area. The system would be reactive, generating interfering signals only in the area where activity is detected. This solution is comparable to hybrid techniques with signal detection and blocking systems.

These solutions analyse all communication attempts (voice, SMS, data), identify the wireless device used and cross-check it in the database of authorised users to accept or deny access to commercial wireless networks. This means that emergency service calls and authorised communications in the prison are not blocked.

One of the major advantages of this solution is that it captures information that can assist the intelligence work of safety agencies. The system can obtain not only the identifying information of the device inside the prison attempting to make the communication, but also the details of the destination of the communication.

The commercial solutions available include devices that carry multiple operators, multiple operating bands and multiple wireless technologies (LTE, UMTS/HSPA, GSM, CDMA, iDEN)¹¹. They offer remote and centralised control, include operation and activity alarms, generate reports automatically and monitor performance indicators.

These solutions have been widely deployed in prisons in the United States and the United Kingdom. The FCC, for example, directly authorises prisons or third parties to operate these types of systems under the figure of operators of Private Mobile Radio Systems (PMRS). This requires an agreement with commercial mobile operators in respect to spectrum use to enable PMRS operators to use licensed spectrum inside the confines of the prison¹².

Because these solutions give access to information relevant to the intelligence work of safety agencies, anyone operating them must work closely with entities involved in prison security. It is, therefore, good practice for the system to be operated directly by the responsible entity or a third party that is qualified and experienced in managing the system and public safety solutions. Deploying a managed access system requires considerable cooperation with commercial operators. PMRS operators need to know about the coverage footprint of commercial networks and the technologies and frequency bands available in each prison where they intend to install the solution. They also need to understand each connection that allows authorised users and emergency calls to access public or commercial mobile communications networks.

As with jammers, these solutions require a detailed engineering study to restrict coverage, as far as possible, to the confines of the prison. Despite this, there is a risk that transmissions will reach beyond the

prison, although they would not directly interfere in communications systems because the signals behave in the same way as commercial network signals. However, except for emergency calls, any user not on the list of authorised users who is “captured” by the system will have their communications blocked. To reduce this risk, the regulatory authority and the PMRS operator can establish a procedure so that individuals who frequent the area near prison boundaries and are not a security risk can be registered on the white list.

The cost of installing Spectrum Management Systems depends on the coverage area, the number of commercial wireless networks and frequency bands carried, and the special functions required. Based on NTIA consultations in 2010¹³, the high cost of these solutions compared to traditional blocking solutions is one of the most challenging aspects for prisons¹⁴.

The main drawback of managed access solutions is that they do not block communications services operating on unlicensed bands, such as Wi-Fi networks.

5.1.3 Dummy cells

Rather than a solution, a dummy cell is a technical alternative that attempts to take advantage of technical aspects of the configuration of mobile stations to “trick” a user’s mobile device.

The user terminal attempts to access communications services through a base station configured so it will not transmit the terminal information. The user may constantly receive “Network busy” messages, or simply not be able to access any service. This solution involves deploying a microcell for each commercial operator, technology and frequency band in the prison, with a distributed antenna system to ensure optimum coverage of the microcell and reduce external base station signals to a minimum. The microcell must also be configured so it will not allow any service.

As with the previous system described, this option also runs the risk of affecting areas outside prisons thus preventing authorised users from accessing communications services. In addition, because a mobile device works by constantly scanning all the base stations that can provide coverage, there may be blind spots where commercial services can be accessed through external base stations. This option does not block technologies such as Wi-Fi, trunking and satellite and provides no information to assist the intelligence work of safety agencies.

11. Characteristics of the Harris CellDefender and ShawnTech Fixed Management Access System solutions.

12. (FCC, 2017)

13. (NTIA, 2010)

14. One of the alternatives suggested to overcome the cost of installing and operating these solutions is to contract a third party to operate the MAS and also provide communications services to corrections personnel.

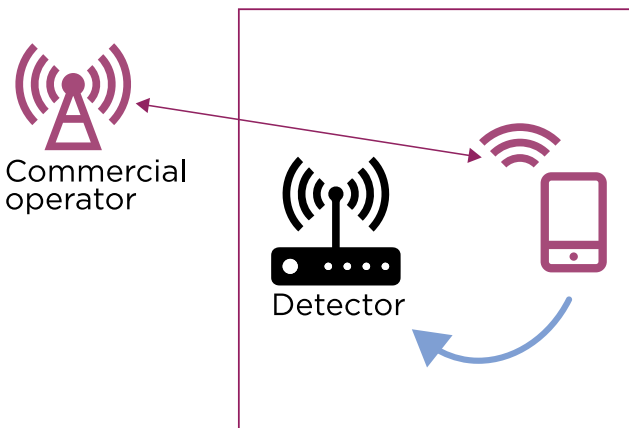
One of the main disadvantages of this option, which makes it impractical to implement, is the administrative and operational complexity of coordinating the blocking of all commercial operators on all frequency bands and in all available mobile technologies.

5.1.4 Techniques based on detection

Detection systems use sensors that locate, trace and identify wireless communications devices inside prisons. In some cases, they detect the generation of radiofrequency signals and determine an approximate location so the device can be seized. A more advanced detector, IMSI Catcher, captures device identifying information (IMEI, SIM Card or IMSI). Devices can then be included in commercial operators’ blacklists (similar to those used to report stolen terminals) and the location can be estimated and the device seized.

Detectors can be portable or fixed, with centralised control¹⁵. The location accuracy of fixed solutions depends on the number of sensors implemented and can reach up to 10 m. These solutions are easily scalable to allow detection of devices operating in any technology and any operating frequency band. Some solutions issue an automatic report of the identifying information of a device, making it easier to include devices on commercial operators’ blacklists. They can also configure a list of authorised devices, which the system detects but does not report.

Because detection devices do not necessarily generate high-power signal transmissions, the risk of interference with communications services beyond prison grounds is significantly lower than with other solutions. However, because detection systems can capture information of all devices within their range, it is important to ensure the sensors are appropriately positioned so they do not report information about devices beyond the grounds of prisons.

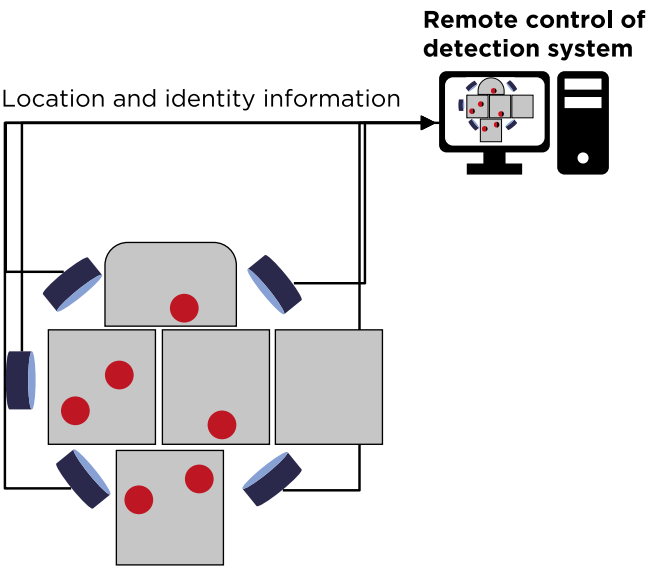


The cost of detection solutions varies depending on their type and complexity. Based on industry replies to the 2010 NTIA consultation, portable solutions are estimated to cost around US\$20,000, while the cost of fixed solutions, which depends mainly on the number of sensors and functions, can range from US\$300,000 to US\$600,000¹⁶.

One of the main concerns with these systems is that signals are not blocked immediately. Offenders may be able to successfully complete an unauthorised communication, creating a potential security risk. In addition, sensors may be vandalised if they are within reach of inmates.

5.1.5 Hybrid solutions

Hybrid solutions are devices that combine two or more of the techniques described. The commercial solutions available include detection and selective blocking solutions using the user’s identification and location , or detection and managed access solutions that provide user location capture, highly accurate device locating, and access control via blacklists (unauthorised users) and white lists (authorised users).



15. Manufacturers such as BLER, Phantom and Prison Jammers have IMSI Catcher detection solutions with differing ranges and accuracy levels.
 16. (NTIA, 2010). These costs refer exclusively to the equipment; costs associated with detection work and operating the system are not included.
 17. Some solutions are offered by PKI (PKI-6210), Phantom Technologies (IMSI Catcher & selective jammer) and BLER.
 18. CellAntenna, CA-STINGER 5G

5.2 Analysis of alternatives

This section analyses the suitability of the technical alternatives described, based on a series of factors.

5.2.1 Effectiveness in blocking unauthorised mobile communications

This factor refers to the ability of the system to block all unauthorised communications originating inside a prison, taking into account the wireless technologies available (2G, 3G, 4G, Wi-Fi, satellite, trunking, WiMax, UHF and VHF) and the areas inside the prison where communications need to be restricted.

5.2.2 Impact on communications services beyond prison grounds or in adjacent bands

This refers to the risk of interfering with communications services beyond the prison grounds or in other frequency bands. It also considers the risk of affecting access to communications services for authorised users.

5.2.3 Deployment and operation costs

These costs refer, firstly, to the potential costs associated with the equipment and the elements of the solution, and secondly, to the complexity of operating the system and its vulnerability to tampering and vandalism, which require repair costs and protection mechanisms.

5.2.4 Support for public safety

The safety factor corresponds to the ability of the system to provide information to assist the work of intelligence and public safety agencies.

The following figure provides a qualitative and comparative analysis of the alternatives described in section 5.1, based on these factors.

FIGURE 14

Comparative analysis of alternative solutions

	 Very good Good Fair Unsatisfactory Deficient					
	Selective jammer	Selective managed access	Selective dummy cell	Detection system	Hybrids	
					Detection + jammer	Detection + managed access
Blocking effectiveness	<ul style="list-style-type: none"> Scalable to all technologies and bands Risk of blind spots 	<ul style="list-style-type: none"> Does not cover Wi-Fi technology Risk of blind spots 	<ul style="list-style-type: none"> Applicable only to cellular mobile networks Risk of blind spots 	N/A Not intended to block communications	<ul style="list-style-type: none"> Scalable to all technologies and bands Risk of blind spots 	<ul style="list-style-type: none"> Does not cover Wi-Fi technology Risk of blind spots
Impact on authorised communications	<ul style="list-style-type: none"> Risk of harmful interference beyond prison grounds Emergency numbers blocked Risk of impact in other bands 	<ul style="list-style-type: none"> Does not generate interfering signals Risk of "capturing" users beyond prison grounds Does not block emergency numbers 	<ul style="list-style-type: none"> Does not generate interfering signals Risk of blocking users beyond prison grounds 	<ul style="list-style-type: none"> Does not generate interference Risk of reporting on users beyond prison grounds 	<ul style="list-style-type: none"> Risk of interference beyond the prison Low risk of authorised users' calls being blocked 	<ul style="list-style-type: none"> Does not generate interfering signals Risk of "capturing" users beyond the prison Does not block emergency calls
Costs and complexity	<ul style="list-style-type: none"> Depends on prison size Risk of vandalism 	<ul style="list-style-type: none"> High cost. Depends on the area, operators, bands and functionalities 	<ul style="list-style-type: none"> Highly complex coordination. Requires multiple solutions for each operator, band and technology 	<ul style="list-style-type: none"> Depends on the type and complexity Risk of vandalism 	<ul style="list-style-type: none"> Depends on the type and complexity Risk of vandalism 	<ul style="list-style-type: none"> High cost
Support for public safety	<ul style="list-style-type: none"> Provides no information 	<ul style="list-style-type: none"> Information about user identification, type of service and receiver 	<ul style="list-style-type: none"> Information about user identification and location 	<ul style="list-style-type: none"> Provides no information 	<ul style="list-style-type: none"> Information about user identification and location 	<ul style="list-style-type: none"> Information about user identification, receiver service and location

Source: BNMC



Based on the comparative overview and good practice identified in the countries surveyed, the following section presents the main conclusions and recommendations of the study.

5.3 Conclusions and recommendations

Using wireless communications devices to organise or commit crimes from prisons, including threats, extortion, kidnapping, murder and escapes, is a reality that affects public safety. This problem requires coordination and cooperation between public protection agencies, prison management, government authorities in the telecommunications sector, and the private sector.

At the same time, public access to communications services is a priority government objective and the basis of the operating principle of radiocommunications systems.

Based on these considerations, the recommendations and the key conclusions of the study are.

- The countries in the region currently addressing this problem have many points in common. Mobile signal inhibitors (jammers) solutions have been deployed in prisons in various Latin American countries, with unsatisfactory results. In nearly all cases, unwanted interference has occurred beyond the prison grounds, equipment has been vandalised, and systems have been less effective than expected. In some cases, contracts with providers of blocking solutions had to be terminated or reworded. Regulations classify unauthorised use of signal blockers that interfere with authorised communications as illegal.
- A study of the laws and regulations of the countries surveyed reveals that, within the framework of the responsibilities of each agency and the regulations applicable to prisons, it is the responsibility of prison management to implement signal blocking solutions. The role of telecommunications authorities is to provide advisory services and develop regulations applicable to the sector, while the role of telecommunications service operators is to cooperate and advise.
- The problem of unauthorised communications from prisons must be addressed across the board. This involves revising security procedures to restrict the entry of communications devices into prisons, blocking or restricting unauthorised communications, detecting and seizing

contraband terminals that have entered prisons, and analysing intelligence information to follow up incidents, identify patterns of behaviour and avoid reoccurrences.

- The technical alternatives available on the market to restrict unauthorised communications from prisons do not perform satisfactorily across the factors analysed. This means that each prison should be studied individually to identify the solution that best meets its needs and priorities. It is also advisable to adopt the good practices for installing radiocommunications systems suggested by the industry and constantly monitor their impact.

The use of jammers should be limited, where possible, to rural areas or locations away from populated areas that could be affected by interference with services. In urban areas it would be preferable to choose solutions that offer greater intelligence in signal analysis, such as managed access or detection systems, to minimise the impact on the surrounding area.

6

References

ANATEL (2002). Resolution 306. Brazil.

ANATEL (2002). Resolution 308. Brazil.

DIARIO OFICIAL DE LA FEDERACIÓN (Mexican Federal Register) (30/09/2012). Guidelines for Collaboration Between Correctional Authorities and Publicly Contracted Telecommunications Service Providers and Technical Specifications for the Installation and Operation of Blocking Systems. (In Spanish). Accessed at http://www.dof.gob.mx/nota_detalle.php?codigo=5266201&fecha=03/09/2012

DIARIO OFICIAL DE LA FEDERACIÓN (Mexican Federal Register) (30/04/2014). 2014-2018 National Public Security Programme (In Spanish). Accessed at http://www.dof.gob.mx/nota_detalle.php?codigo=5343091&fecha=30/04/2014

DIARIO OFICIAL DE LA FEDERACIÓN (01/08/2016). TECHNICAL PROVISION IFT-010-2016. Accessed at http://dof.gob.mx/nota_detalle.php?codigo=5446400&fecha=01/08/2016

DIARIO OFICIAL DE LA FEDERACIÓN (Mexican Federal Register) (14/07/2014). Federal Telecommunications and Broadcasting Act. (In Spanish) Accessed at http://www.dof.gob.mx/nota_detalle.php?codigo=5352323&fecha=14/07/2014

ECONOMÍA Y NEGOCIOS (27/08/2016). Gendarmerie consults on technology available to block mobile phones in prisons. (In Spanish) Accessed at <http://www.economiaynegocios.cl/noticias/noticias.asp?id=284125>

ESTADO MAYOR (Joint Chiefs of Staff) (22/09/2013). Inmates Unblock Mobile Signal. (In Spanish) Accessed at <http://www.estadomayor.mx/33404>

FEDERAL COMMUNICATIONS COMMISSION (May 2017). Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities. Accessed at <https://www.federalregister.gov/documents/2017/05/18/2017-09885/promoting-technological-solutions-to-combat-contraband-wireless-device-use-in-correctional>

GLOBO - EPOCA NEGOCIOS (23/01/2017). Only 23 prisons in São Paulo have a mobile phone jammer. (In Portuguese) Accessed at <http://epocanegocios.globo.com/Brasil/noticia/2017/01/so-23-prisoos-tem-bloqueador-de-celular-em-sao-paulo.html>

LA JORNADA (25/03/2015). Kidnappings from Correctional Facilities. (In Spanish) Accessed at <http://www.jornada.unam.mx/2015/03/25/politica/008n1pol>

NATIONAL PENITENTIARY AND PRISON INSTITUTE (19/07/2012). Transitory Directive 022/2012 to Prevent and Control Extortion Originating in Correctional Facilities. (In Spanish) Accessed at http://www.inpec.gov.co/portal/page/portal/INPEC_CONTENTIDO/NORMATIVIDAD_INTRANET/DIRECTIVAS_PORLET/DIRECTIVA22.pdf

NATIONAL PENITENTIARY AND PRISON INSTITUTE (11/02/2016). Signal Blocking and Inhibiting System. (In Spanish) Accessed at http://www.inpec.gov.co/web/guest/estadisticas/-/document_library/TWBUJQCWH6KV/view_file/49159

NATIONAL TELECOMMUNICATIONS AGENCY - ANATEL (2002). Resolution 306. Brazil

NATIONAL TELECOMMUNICATIONS AGENCY - ANATEL (2002). Resolution 308. Brazil

NATIONAL TELECOMMUNICATIONS AND INFORMATION COMMISSION (2010). Contraband Cell Phones in Prisons.

PKI-ELECTRONICS (2017). Intelligent Cellular Jammer with Detector. Accessed at <http://www.pki-electronic.com/products/jamming-systems/intelligent-cellular-jammer-with-detector/>

SENATE OF THE REPUBLIC (14/03/2017). MOTION FOR RESOLUTION. (In Spanish) Accessed at http://sil.gobernacion.gob.mx/Archivos/Documentos/2017/03/asun_3507338_20170323_1490203162.pdf

Annex 1

Case studies

The following infographic summarises the key aspects of the results observed after mobile signal inhibitors (jammers) were installed in two prisons in Colombia. The first is in the semi-urban area of Picaleña, near the city of Ibagué, and the second is in Bogotá.

The analysis was prepared using measurements and a statistical report issued by mobile operators in Colombia.

Case studies I

Picaleña prison (Ibague - Colombia) 1/2

Semi-urban location
Approx. area 24 ha

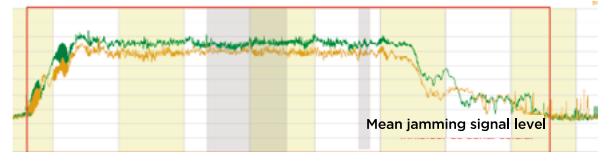


Installation of signal blocker as part of INPEC "Plan Cerrojo", 2013

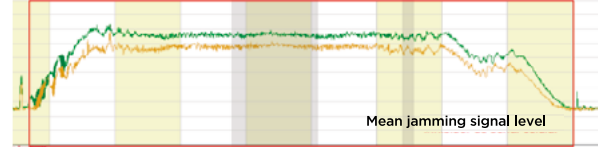
INPEC tests → 100% of calls blocked inside prison

Operator tests (20 calls) → All calls blocked. No 3G/4G operator signals identified

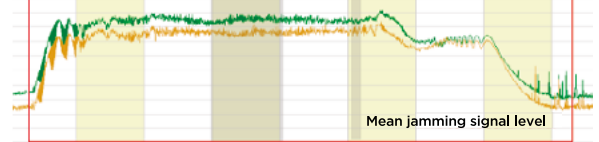
50m from prison grounds



120m from prison grounds

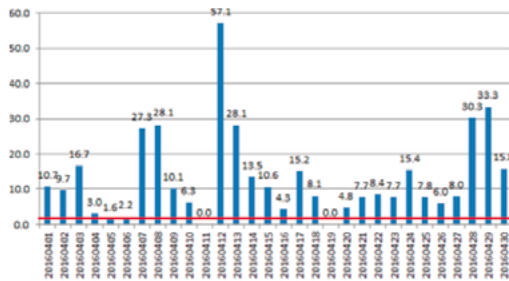


200m from prison grounds



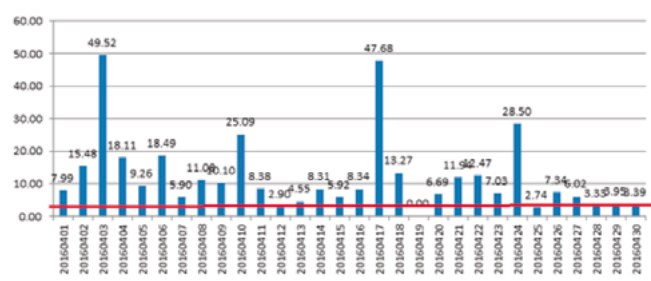
The high levels of interference drastically affected user quality of service.

% 2G dropped calls April 2016



Dropped calls rose from a 2% average to more than 20% (50% during high traffic)

% unsuccessful 3G call attempts



Dropped calls rose from a 3% average to more than 11% (47% during high traffic)

8. (INPEC, 2012)

Case studies II

La Picota Prison (Bogota - Colombia) 2/2

Urban location
Approx. area 40 ha

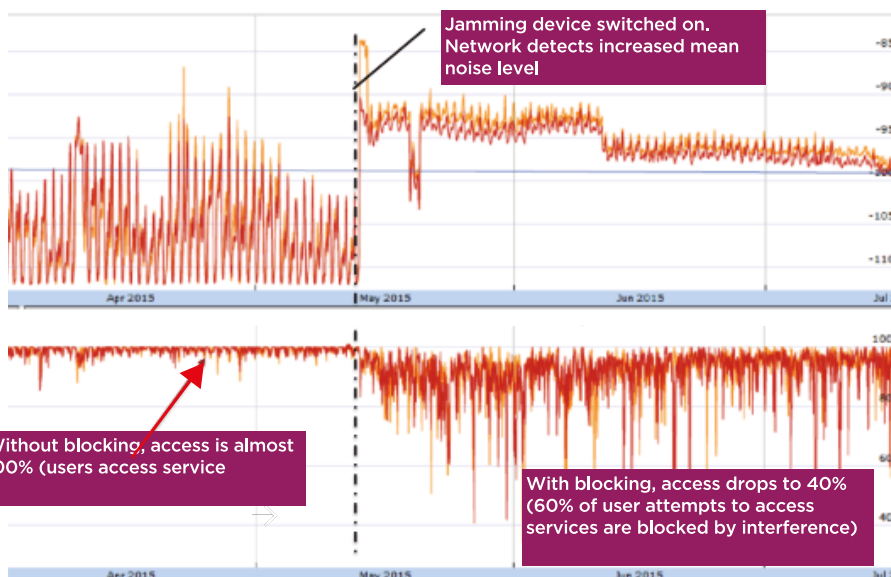


Jammer installed under INPEC "Plan Cerrojo", 2013

INPEC tests → 50% of calls blocked inside prison
 Operator tests (20 calls) → All calls blocked. No 3G/4G operator signals identified

The signal/interference ratio is at deficient levels around the prison

Jamming uplink frequencies has a greater impact on overall performance of the affected base station



Annex 2

Regulatory framework on the use of signal blockers

I. Mexico

Public safety agencies in Mexico consider it a priority to combat offences such as extortion, threats and fraud committed by telephone from inside prisons. Figures reported by state attorneys and prosecutors reveal more than 400 cases of extortion and kidnapping a month¹⁹. The recitals of government regulations acknowledge that “offences are carried out from inside prisons in coordination with criminal gangs on the outside, including extortion with the threat of kidnapping or death, as well as telephone fraud against society (...)”, in addition to intimidation of inmates’ relatives, witnesses or corrections personnel, and even compilation of photographic material to prepare escapes or mutinies²⁰.

Article 149 of the General National Public Security System Act (2009) states: “the National Council shall determine the cases, conditions and requirements for blocking cellular telephone signals in strategic prisons to ensure public safety”, under the responsibility of the Public Safety Agencies that make up the National Council.

In 2011, the Government of Mexico City contracted the firm Software DSI under the terms of the 2009 legislation to install and operate 155 jammers in six Mexican prisons, at an approximate cost of US\$1.9 million²¹. The strategy did not have the desired outcome because of the limited effectiveness of the systems at blocking calls. It was also suspected that inmates and prison guards had tampered with the blocking devices²². The contract was terminated in 2013.

A regulation issued in 2012 outlined the *Guidelines for Collaboration between Correctional Authorities and Publicly Contracted Telecommunications Service Providers and Technical Specifications for the Installation and Operation of Blocking Systems*, which define the obligations for all agencies that administer

social reintegration centres or juvenile detention prisons and providers of telecommunications services to disable or cancel “on a permanent basis, cellular telephony signals, radiocommunication signals and data or image transmission within the confines of social reintegration centres, prisons (...), with the requirement that such action does not extend more than 20 metres beyond the grounds of the prisons (...)”²³.

The regulation also states that all prisons must have equipment to permanently block mobile telephone signals and set up mechanisms to prevent and remedy undesirable effects on mobile service users. It defines the roles of each agency involved, mandatory technical specifications of devices, and device monitoring.

The following figure summarises the obligations of each party.

19. In January and February 2015, 826 cases of extortion and kidnapping were reported (LA JORNADA, 2015).

20. Recital of the Regulation Guidelines for Collaboration between Correctional Authorities and Publicly Contracted Telecommunications Service Providers and Technical Specifications for the Installation and Operation of Blocking Systems. From National Congress on the Penitentiary System, Mexico. (DIARIO OFICIAL DE LA FEDERACIÓN, September 30th 2012).

21. Press release (ESTADO MAYOR, 2013). The 155 devices were purchased for 24.79 million Mexican pesos (approximately US\$1.9 million at an exchange rate of 13 pesos a dollar).

22. Comments made in the Motion for Resolution Respectfully Asking the National Congress on the Penitentiary System and the National Public Security System, in Accordance with the General Public Security System Act, to Strictly Comply with the Provisions of Article 31 of the Act of the Senate of the Republic of March 2017. (SENADO DE LA REPÚBLICA, 2017).

23. Recital of the Regulation Guidelines for Collaboration between Correctional Authorities and Publicly Contracted Telecommunications Service Providers and Technical Specifications for the Installation and Operation of Blocking Systems. From National Congress on the Penitentiary System, Mexico. (DIARIO OFICIAL DE LA FEDERACIÓN, September 30th 2012)

FIGURE 15

Obligations of the parties involved - Mexico

Secretariat of Public Security (Undersecretariat of the Federal Penitentiary System) Supervise compliance with decision

- **National Congress on the Penitentiary System**
Coordinate between the Executive and the Federal District, promote decisions, request quotes
- **Decentralised Administrative Agency for Prevention and Social Reintegration (Federal Level)**
Provide and ensure installation and operation of signal blockers
Supervise functioning (20m limit beyond prison grounds)
Directorates General – State and Federal District
Provide and ensure installation and operation of signal blockers
.....Supervise functioning
Penitentiary centre management
Prepare area for installation. Surveillance and reports
- **Operating, monitoring and remote supervision centres**
Supervise installation. Operate and monitor signal blockers and ensure functionality

Secretariat of Communications and Transport

Advise

- **Federal Telecommunications Institute (Formerly COFETEL)**
Support corrections authorities, coordinate with public contractors, monitor quality of service
- **Technological Development Directorate**
Advise on technical requirements, remedy incidents affecting the surrounding area and identify new solutions
- **Public contractors providing telecommunications networks**
Collaborate in blocking signals in all frequency bands. Carry out regular testing. Support functionality monitoring. Study new solutions

Source: (DIARIO OFICIAL DE LA FEDERACIÓN, 2012)

To strengthen this government objective, the strategies defined in the 2014-2018 National Public Security Programme included adopting actions to “break the link between inmates and criminal organisations inside and outside prisons”²⁴. The first line of action defined was implementing effective measures to block mobile signals. In June 2017 an amendment of the National Public Security System Act implemented the following obligations regarding the use of jammers:

Article 7: (...) Federal District, State and Municipal Public Security Agencies, within their competences and in accordance with the provisions of this law, must coordinate to:

(...)

XII. Ensure that **all centres** for social reintegration, prisons and juvenile detention centres, whether federal or under the authority of federal entities and by whatever name they are known, **have equipment to permanently block or cancel mobile telephone signals**, radiocommunication signals and data and image transmission within their boundaries;

Article 31: (...) functions of the National Penitentiary System Congress:

(...)

VIII. Draw up guidelines so that the federation and federation entities comply, within their competences, with the obligation to **acquire, install and maintain operational, equipment to permanently block or cancel mobile telephone signals**,

radiocommunication signals and data, voice and image transmissions inside social reintegration centres, prisons and juvenile detention centres, whether federal or under the authority of federal entities and by whatever name they are known.

*This equipment **shall be operated by authorities other than those of the prisons, at external locations.** It shall include automatic systems to send alarm signals whenever functionality is interrupted and shall be monitored by the National Public Security System, with the collaboration of public contractors for public telephone networks.*

*The signal blocking referred to in this article shall be carried out in **all frequency bands** used to receive signals on mobile communications terminals **and under no circumstances shall it have any effect more than 20 metres beyond the grounds** of prisons or establishments, in order to guarantee the continuity and the safety of services for external users.*

Article 190 of Mexico’s Federal Telecommunications Law states that contractors providing public telecommunications services have the obligation to “collaborate with the corresponding authorities to enable, in the technical and operational field, permanent cancellation or disabling of cellular telephone signals, radiocommunication signals and data and image transmission inside the confines of social reintegration centres, prisons (...)

24. Strategy 6.3. of the 2014-2018 National Public Security Programme of the Mexican United States (FEDERACIÓN, 2014).

Collaboration by public contractors must include the technical factors of replacement, maintenance and servicing. (...) are obliged to collaborate with the National Public Security System in monitoring the functionality or operativity of the equipment used to permanently block cellular telephone signals (...)”²⁵.

In view of the provisions of the Law, and after the Federal Telecommunications Institute (FTI) issued its Guidelines for Collaboration in Security and Justice Matters in November 2015, the FTI published Technical Provision IFT-10-2016 in August 2016 on the characteristics and requirements for mobile telephone signal blocking equipment in prisons and other establishments.

The Provision includes the following considerations:

- The use of signal blocking equipment is restricted to within the boundaries of prisons. No other use is permitted;
- The equipment must have separate adjustable power for each frequency band;
- The use of external power amplifiers for blocking equipment is not permitted;
- The equipment must have no visible controls, to avoid tampering;
- The equipment may block only in the frequencies corresponding to the downlink (i.e., from the network to the mobile terminal);
- Blocking is not permitted in the 380 to 399.99MHz band, which is used for public safety applications;
- Equipment must comply with electromagnetic field exposure limits; and
- Equipment must be type approved in specialised laboratories.

II. Colombia

Kidnapping and extortion are the offences that cause most concern for public safety agencies in Colombia. Decree 4768/2011, “*adopting measures to restrict the use of telecommunications devices in correctional and prison facilities (...)*”, states that inmates cannot possess private communication devices²⁶, while acknowledging a significant increase in offences committed from inside prisons, such as threats, scams and extortion, using communications devices.

The Decree created a regulatory framework in the following three aspects:

1. It empowered the Ministry of Information and Communications Technologies (ICT Ministry) to authorise the National Penitentiary and Prisons Institute (INPEC) to “*inhibit or block the transmission, reception and control signals of providers of mobile telecommunications networks and services (...)*” in prisons where there are clear indications of offences being committed from inside using communications devices.

It is the responsibility of the INPEC to apply to the ICT Ministry, outlining the technical conditions applicable to the measure, and to operate the signal blocking equipment while avoiding impact on outside areas. The National Spectrum Agency is responsible for monitoring compliance with this obligation.

It is the responsibility of the INPEC to apply to the ICT Ministry, outlining the technical conditions applicable to the measure, and to operate the signal blocking equipment while avoiding impact on outside areas. The National Spectrum Agency is responsible for monitoring compliance with this obligation.

2. The ICT Ministry, after receiving a technically detailed application from the INPEC, may order the providers of telecommunications networks and services to eliminate or restrict their transmission, reception and control signals in the prisons identified. Telecommunications operators are responsible for operating the infrastructure required to restrict their signals, while avoiding impact on areas beyond the prison. The ICT Ministry is responsible for monitoring compliance with this obligation.
3. Compliance with quality of service indicators does not apply in prisons affected by these measures. Under this framework, the INPEC prepared an action plan based on the following areas²⁷:
 - Manage the assignment of mobile telephony signal blockers or inhibitors. A total of 16 prisons were identified. Round tables were held with operators and the government entities involved, to define coverage adjustments to minimise the impact beyond the grounds of the prisons; and

25. (DIARIO OFICIAL DE LA FEDERACIÓN, 2014)

26. Article 111 of Law 65/1993

27. Transitory Directive 022/2012 to Prevent and Control Extortion Originating in Correctional Facilities. (INPEC, 2012)

28. Incluye los centros de reclusión identificados en el Plan Cerrojo (11 centros), Orion (1 centro) e Institucional (5 centros).

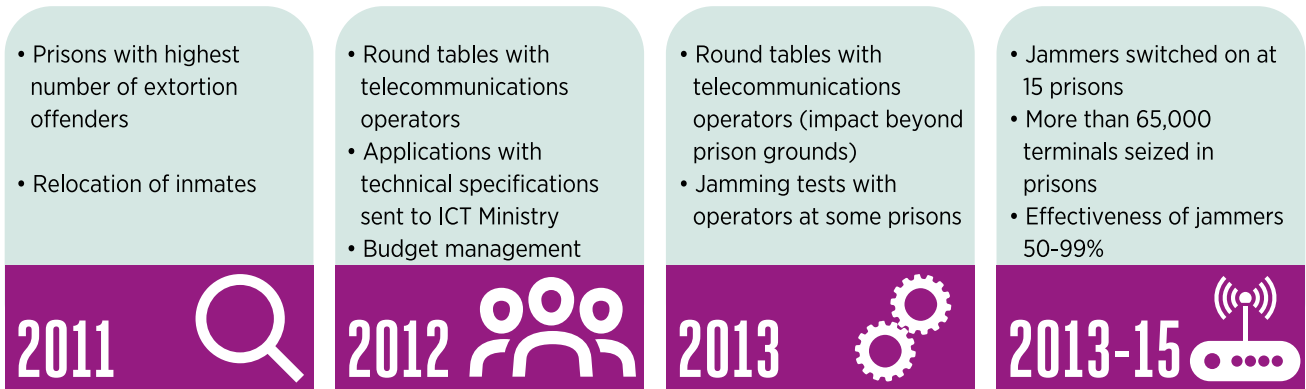
- Review the procedures for controlling the entry of mobile phones into prisons and their seizure. In recent years the INPEC has worked with the National Police Anti-Kidnapping and Anti-Extortion Directorate to use tactical devices capable of identifying SIM numbers (IMSI) and mobile device codes (IMEI) so they can be blocked by mobile operators;
- Monitor inmates associated with extortion offences, with the option of transferring them to prisons where signal blocking measures are in place; and

- Cooperate with national and regional crime prevention entities. In 2016 the INPEC reported the results after the working plan had been implemented.

The following figure outlines the most significant features of the report.

FIGURE 16

INPEC Action Plan - Colombia



Source: BNMC

After testing at the 15 prisons, where jammers had been installed by the end of 2015, it was found that call blocking effectiveness was less than 85% in four cases, 85% to 95% in five cases and more than 95% in seven cases. However, in more than 70% of cases problems were experienced with tampering or vandalism, and there was significant impact on the quality of communications services in areas beyond the grounds of the prisons.

Based on Decree 4768/2011, in August 2013 the ICT Ministry issued Resolution 2774, “governing the use of radio signal inhibitors, blockers and amplifiers”, which determined the following in relation to the use of jammers.

- Using jammers without the required authorisation and in the cases included in Resolution 2774/2013 are clandestine uses of spectrum, to which the sanctions and procedures laid down in the ICT Law of Colombia shall apply.
- Authorisation may be requested for the installation and operation of jammers in fixed, confined locations only by public or financial entities on the grounds of safety or general interest. In this case an application must be submitted, with the specifications of the equipment, design and coverage map inside and 500m beyond the premises. Equipment must comply with electromagnetic field exposure limits.
- When the area beyond the premises is affected, the jammer must be switched off until the problem is remedied.
- Security agencies of the State of Colombia may use fixed or mobile jammers in fixed, confined locations or in open locations exclusively for public safety, without the need to obtain permission from the ICT Ministry.

III. Brazil

In 2002, Brazil's National Telecommunications Agency (ANATEL) issued two Resolutions governing the use of signal blocking devices. The first of these, Resolution 306/2002, passing the "*Regulation for certifying and approving radiocommunication signal blockers*", defined the following requirements for these devices.

- They must block frequency bands corresponding to telecommunications services;
- They must not block telecommunications signals beyond the established limits;
- They must permit blocking of the signals of any technology used to provide telecommunications services;
- They must include power control for each frequency band; and
- They must comply with electromagnetic field exposure limits.

The second regulation, Resolution 308/2002, governs the use of radiocommunication signal blockers. It authorises their use in prisons after an application made to ANATEL with a clear technical project indicating the frequency bands targeted for blocking. The resolution also requires coordination and permanent contact with telecommunications service operators and ANATEL.

These regulations define the obligations for each party involved. The most important of these are:

- Telecommunications service operators are obliged to maintain strict confidentiality regarding the information provided to them about signal blocking equipment. They must also notify the parties concerned about changes to their networks that may affect the coverage footprint in the area targeted for signal blocking and report disruptions in the service in areas beyond the established limits;
- ANATEL must comply with confidentiality of information requirements, monitor compliance with regulations and support the National Penitentiary Department (DEPEN) by providing the information required for the design of the technical specifications of the blocking solution; and

- Entities authorised to install and operate signal blocking equipment must provide detailed technical specifications, maintain contact and coordinate with telecommunications operators and ANATEL, and use equipment certified as complying with current regulations, installed out of reach of inmates. Telecommunications service in areas beyond the grounds of the prison must not be affected (this carries the obligation to coordinate with operators for impact evaluation at test points).

Press articles estimated that 23 prisons in São Paulo have signal blocking devices, corresponding to 14% of all prisons in the area²⁹. However, mobile terminals continue to be seized in prisons equipped with a jamming system, indicating that the solution is not 100% effective.

The authorities and the general public are aware that communications services beyond prison grounds are affected. To tackle this, it was suggested that responsibility for installing and operating signal blocking systems should be transferred to telecommunications service operators. However, considering that public safety is a state duty, and in view of the procedures and responsibilities defined in Brazil's Criminal Enforcement Law, the Federal Supreme Court ruled in a decision on 3 August 2016 that this proposal was unconstitutional.

IV. Chile

As in other Latin American countries, the use of terminals for mobile communications inside prisons to commit offences is a critical priority issue on the agenda of safety agencies. According to estimates, nearly 156,000 terminals were seized inside prisons in Chile from 2011 to 2016³⁰.

Chilean Gendarmerie is responsible for regulating and monitoring the installation and operation of signal blocking devices in prisons. It is advised by the Undersecretariat of Telecommunications (SUBTEL) in matters associated with instrumental and regulatory capacities.

In 2012 a public tender was launched for installation of mobile signal blocking systems in six Chilean prisons. The procedure required the successful company to implement a solution that offered i) total restriction of unlawful communications generated in prisons, ii) no interference with Gendarmerie internal communications, and iii) no impact on communications beyond prison grounds.

29. Estimated investment of 31 million Reales (GLOBO - EPOCA NEGOCIOS, 2017).

30. <http://www.economiaynegocios.cl/noticias/noticias.asp?id=284125>

The contract was awarded to Telefónica Móviles, but the results of the solution were unsatisfactory because it was impossible to meet all three objectives. This led to early termination of the contract.

In recent years, Chilean Gendarmerie has requested information from the industry about solutions for blocking wireless communication signals inside prisons, with a view to launching another public tender.

IV. United States

The United States Federal Communications Commission (FCC) has regulated and explicitly notified the prohibition on selling, manufacturing, marketing, importing, operating and using devices that block, inhibit or intentionally interfere with authorised radiocommunication systems such as mobile telephony, police radar, GPS and Wi-Fi systems³¹.

The main reason for the measure adopted by the FCC is that the use of these devices not only affects authorised radio communication services, but also poses serious risk to public safety communications, including public calls to emergency services. The primary mission of the FCC is to advance the goals of universal service.

Section 2.807 of the Commission regulations includes exceptions to these prohibitions. Jamming devices may be manufactured solely for export or the use of the Government of the United States or any of its agencies, provided it has been authorised by the Commission.

The Government of the United States also recognises that it is necessary to combat contraband use of wireless communications devices inside prisons. According to the Federal Bureau of Prisons (BOP), 8,700 mobile phones were recovered in federal prisons from 2012 to 2014, and in 2013 the California Department of Corrections and Rehabilitation confiscated 12,151 phones³². Numerous cases were reported of offences being committed using mobile phones.

To tackle this problem, some prisons have implemented radio-based technologies to detect and block wireless communication devices inside their boundaries. These technologies are known as Contraband Interdiction Systems (CISs) and require FCC authorisation. Round tables have been held to identify alternative solutions.

The technologies used in United States prisons fall into two categories: i) managed access and ii) detection. The following figure describes the main features of each type.

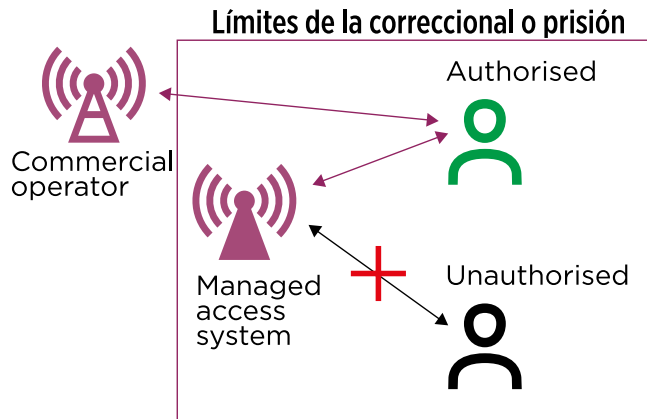
31. FCC - Jammers Enforcement (<https://www.fcc.gov/general/jammer-enforcement>). Section 301 of the Communications Acts states that no person shall operate any apparatus for the transmission of signals by radio without authorisation. Section 303 states that no person shall wilfully or maliciously interfere with any authorised radio communications.

32. Report and Order and Further Notice of Proposed Rulemaking - GN Docket 13-111 (2017). (FCC, 2017).

FIGURE 17

Technologies used to combat the use of wireless devices in prisons - USA

Managed access system



Micro-cellular private network operating on spectrum licensed to commercial operators. Requires FCC authorisation

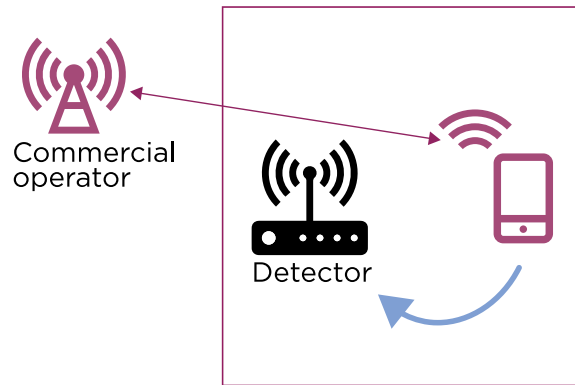
Analyses transmissions to and from mobile terminals
Restricts unauthorised users and allows authorised users to connect to commercial networks

Cross checks user identifying information with a list of authorised users

Does not interfere with 911 calls

Source: Based on (FCC, 2017)

Detection



Locates, tracks and identifies radio signals originating from a device

- Passive: Detects radio signals
- Active: Obtains user identifying information (IMSI/IMEI) for inclusion in blacklists

Does not require FCC authorisation

For installation of managed access solutions, the FCC must study and authorise an award or loan of spectrum by telecommunications operators to entities operating this solution inside prisons. It is estimated that managed access solutions have been tested and/or deployed in 52 prisons in 17 states.

In March 2017, the FCC announced a series of initiatives to promote technological solutions to combat the use of contraband wireless devices smuggled into prisons. The initiatives were based on the following considerations:

- Simplify FCC authorisation procedures for the installation of CIS solutions in prisons. This includes the process for awarding spectrum between telecommunications service operators and MAS operators.
- Cooperation from wireless communications service operators; and
- Appointment of a person from the FCC specifically to deal with issues associated with these procedures; i.e., a figure similar to an ombudsperson.

VI. United Kingdom

It is important to note that the Wireless Telegraphy Act 2006 prohibits the installation of wireless devices in the UK mainland, Northern Ireland and territorial waters, the Isle of Man and the Channel Islands without a licence obtained from the Office of Communications (Ofcom) and compliance with its requirements. The use of equipment that interferes with or blocks communications signals, with the risk of affecting emergency communications, is unlawful³³.

Security agencies report that unauthorised telephones are being used in prisons by organised criminal gangs to import weapons and drugs, coordinate escapes and carry out murders. The National Offender Management Service (NOMS) estimates that 7,400 SIM cards were seized in prisons in England and Wales in 2013 and 2014³⁴. These results have been reported even though testing of mobile signal inhibitors was initiated in 2012 in 10 UK prisons.

Once the problem was identified, techniques were deployed to detect wireless devices. In 2015 telecommunications operators were compelled to disconnect terminals and SIM cards reported by county courts as unauthorised for operation inside prisons. The courts would not be required to be in physical possession of the devices, which could instead be detected using electronic mechanisms.

³³. <https://www.ofcom.org.uk/spectrum/radio-spectrum-and-the-law/jammers>

³⁴. Serious Crime Act 2015



GSMA HEAD OFFICE

Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601

GSMA LATAM

Av. Del Libertador 6810,
piso 15
Buenos Aires, C1429BMO,
Argentina
Tel: +54 (11) 5367 5400