STEMMING THE FLOW

Andy Gent *examines the problem with illicit mobile phones in prisons and reveals a potential solution*

Contraband mobile phones have long been a security and public safety concern in prison and detention facilities around the world. While some prisoners may use these mobile devices for communicating with loved ones, others use them to continue their illegal activities. Almost daily, prisoners are using illegal mobile phones to facilitate a wide range of criminal activity from behind bars including drug supply; large-scale fraud; harassment of witnesses; procurement of firearms; and perhaps most worryingly, maintaining and enhancing the influence of prisoners convicted of terrorism offences.

Last year in the UK, a terrorist who attempted to murder a prison officer at maximum-security prison HMP Whitemoor uploaded an image of himself on social media, boasting that he would be home soon. The fact that one of these terrorists had a mobile phone and unconstrained access to the outside world within a maximum-security prison is a huge cause for concern and could have provided him with continuous access to extremist material.

As technology has evolved, mobile devices have become physically smaller and more advanced – making them easier to smuggle into prisons. Convicted criminals and their accomplices use a variety of methods to smuggle illicit mobile phones into prisons; through visitors, post, corrupt prison guards and bizarrely, within a tennis ball thrown over the perimeter fencing or by using drones to drop them over the prison walls.

PHONE JAMMING HAS BECOME OUTDATED; A MORE CONSIDERED STRATEGY IS REQUIRED

Almost 12,000 contraband mobile phones were found in prisons in England and Wales last year, up three percent on the previous year. With the current prison population in England and Wales at approximately 80,000 prisoners, that equates to roughly one phone for every six inmates.

The problem of illicit mobile phones is not restricted to the UK. In the first half of 2017 alone, France seized more than 19,000 phones in its prisons, an average of almost one mobile phone for every three inmates. And in Puerto Rico, contraband mobile phones were used to coordinate a fatal attack on a corrections officer.

A combination of expensive call rates and limited access to private phones in prisons makes illicit mobile phones valuable commodities. In UK prisons, they can cost anywhere between £400 and £1,000 just to borrow. Being in possession of a phone therefore puts an inmate in a position of power in the prison hierarchy, and can contribute to increased violence and create further safety issues for security staff and other prisoners.

Gang activity can also inevitably be facilitated much easier when incarcerated members have access to mobile phones. In Brazil, for example, gang leaders orchestrated large synchronised riots in over 70 prisons simultaneously in 2006. If communications between gang members are cut off or monitored this can hinder their ability to commit such violent acts and provide important intelligence to the prison services.

In a bid to tackle the problem of illicit mobile phones in prisons, laws have been passed in various jurisdictions, placing penalties on inmates who possess mobile devices as well as staff who smuggle them in.

In 2018, the UK Government announced plans to install in-cell phones in 20 prisons in England and Wales to tackle the flow of illegal handsets and reduce tension on wings. However, all calls are recorded, and calls can only be made to a small list of pre-approved contacts. This makes it likely prisoners with the intention to use contraband mobile phones to carry out criminal activity will continue to try and smuggle them in.

Many prisons carry out physical searches on prisoners to check for contraband on arrival as well as frequent searches of cells. Similarly, visitors often have to pass through body scanners to check for contraband. However, prisoners are continuously finding innovative ways to get illicit mobile phones, drugs and contraband inside. To finally put an end to this epidemic, a new approach is needed, and technology holds the answer.

Many prisons around the world have traditionally used a method known as phone or signal jamming to block communications from inmates and tackle the issue of contraband mobile phones. This approach works by transmitting a blocking signal to prevent the handset receiving its base station signal.

The legislation surrounding phone jamming varies from country to country. In the US, for example, Federal law bans the use of such technology by state agencies, and it is opposed by the wireless industry. Instead, a more targeted approach is preferred. Whereas in Ukraine, signal jamming is legal, and it has been suggested for the technology to be used in schools. Meanwhile, in the UK, the installation and use of signal jammers in prisons has been legal since the end of 2012.

Current figures suggest there is roughly one illicit mobile phone for every six inmates

Phone jamming comes with inherent weaknesses: it's a blanket approach, all phones and SIM cards within a jammer's radius will have their mobile reception blocked, and crucially jamming fails to build any intelligence and insights around illegal activity taking place inside and beyond the prison walls. Phone jamming is an outdated approach; a more targeted and considered strategy is required.

To understand the full picture of illicit mobile use in prisons and identify and prevent criminal activity, prison security teams need to gather social intelligence on the patterns of behaviour around these illegal communications. This can include how devices and SIM cards move through a prison and monitoring which inmates have control of the device. To avoid detection, the SIM card, the battery and the device are usually distributed within the prison to mitigate risk of loosing the entire device in unexpected raids.

Staff then have the insight to undertake in-depth analysis of the communications to support possible ongoing criminal investigations and take positive action by intercepting the calls. Depending on the laws of the land and following ministerial authorisation, prison officers can now also use IMSI and Wi-Fi-catcher technology to identify the location of contraband mobile phones, down to the precise cell.

An IMSI is a 15-digit number assigned to the SIM card, which is unique to a subscriber and identifies each mobile user within the network. Every SIM card is assigned a unique number to ensure network providers receive payment for all calls made, even if the SIM card is used in multiple handsets. An IMSI-catcher works

▶

by mimicking a phone base station and fooling nearby mobile phones into connecting to it, meaning prison officials can gain access to these IMSIs.

By default, smartphones are constantly searching for a Wi-Fi connection when switched on and Wi-Fi is enabled; meaning Wi-Fi-catchers can identify any contraband mobile phones within the prison site quickly and effectively. A network of IMSI and Wi-Fi-catchers can be deployed permanently within a prison environment, with the capability to define zones. This allows prisons to target specific areas within the prison and means residents who live near the prison feel safe in the knowledge their phones will not be picked up and consequently monitored.

> MOBILE DEVICES HAVE BECOME MUCH SMALLER, MAKING THEM EASIER TO SMUGGLE INTO PRISONS

There has been an ongoing debate surrounding the ethics of using interference technology such as IMSI and Wi-Fi-catchers, with critics arguing they are an invasion of privacy. But prisons are unique environments and legislation has long been in place making the possession of a mobile phone illegal behind the prison walls. The invasion of privacy argument, while being an important consideration, does not trump the prison's duty to protect the public; in particular when it comes to national security, the safety of prison staff and fellow prisoners and the reputation of the prison service.

One of the main issues associated with this type of technology relates to the privacy of surrounding residents and fears of their phones also being monitored. In the UK, the Prisons Act 2012 meant fake base stations such as IMSI-catchers could only be deployed within prison walls. However, amendments to the bill in 2017 authorised mobile network operators to deploy interference devices to monitor the use of mobile phones in prisons, which has raised concerns about the relaxed rules around the location of IMSI-catchers.

While IMSI or Wi-Fi-catchers could only be used in a fixed place in the past, the miniaturisation of technology has meant that now they can be made portable and more targeted to specific areas of prisons. This means prison officials have greater control over where devices are monitored and the areas outside the prison complex such as car parks, access roads or residential areas are not affected.

There is no one-size-fits-all approach to eradicate the use of illicit mobile phones and improve wider prison security. As pressure mounts on prisons to handle the flow of contraband entering, a multi-layered and holistic approach is needed – encompassing innovative mobile technologies, CCTV, door access, visitor management and comprehensive training.

As security technologies evolve, so do the prisoner's attempts to smuggle in contraband. For that reason, blanket measures such as phone jamming are unsustainable and ineffective in today's digital communications landscape. An effective prison security system relies on leveraging innovative technologies and seizing new opportunities to counteract the continuous efforts of prisoners to breach security inside and outside of the prison walls.

The technology to enable prisons to monitor illicit communications and pinpoint mobile phone use to precise cells already exists, but is not being used to its full potential. A lack of funding for prison security and legislation surrounding the use of surveillance technology are two huge barriers putting a stop to this, and that needs to change if countries are going to be able protect guards, other inmates and the public at large ●

Andy Gent is CEO of Revector, a global leader in telecoms intelligence for fraud prevention and security.

Phone jamming fails to build any intelligence and insights around illegal activity taking place inside and beyond the prison walls