A response to counter
Cellular Coms & Wireless Data Vulnerability:
IJS-6100 Detector Jammer

Prepared by
Homeland Security Strategies GB Ltd.

Problem: Cellular Voice & Data Handsets pose a threat to High Level Security & Privacy

Solution: The Detector Jammer - Detect, Locate, & Neutralize unauthorized cellular activity using Communication Control

The Detector Jammer is a hybrid of integrated technologies consisting of a Control Center, deployed detection sensors (overt or hidden), and RF Jamming architecture to:

- **Detect Cellular Voice and Data Communications**
- **Alert the operator of unauthorized communications in process**
- **When activated, the operator can deny communications through active RF Jamming**

The active RF Jamming can be curtailed at neighboring room borders through the implementation of RF shielding.

Theory of Operation

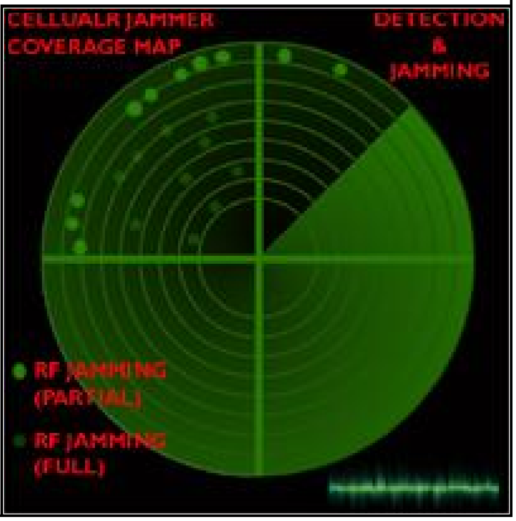
The Detector Jammer is a system that is designed and deployed for the Detection and Jamming of Cellular Voice and Voice-Data driven Wireless 'SmartPhones' - PDA related devices (ex: BlackBerry & iPhone).

It is made up of attuned telemetry that integrates radio receiver and RF Jammer hardware with proprietary intelligent communication processors that can operate autonomously or manually by the operator 24/7. There is no daily start-up time or boot-up delay, as the system is continually active non-stop.

The Detector Jammer configured in a conference room to combat unauthorized communication use.

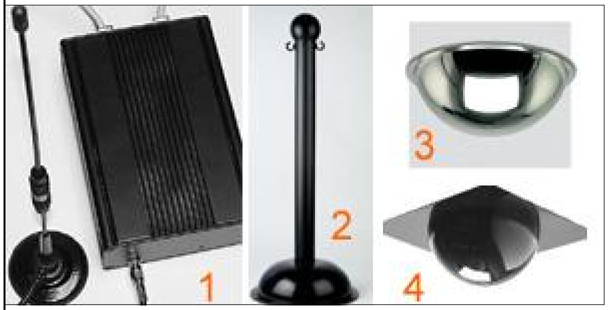
Pre-Design Factors - System architecture is made up of 3 individual components:

Software Logic Program: a proprietary communication database of signal traffic pathways that are preset as well as amendable by the user
Sensor Equipment: Hardware that can operate autonomously and in cohesion with the Graphic User Interface (GUI).
Communication Jamming Emission Module: Used to disable communication links automatically or by manual control within selectable user defined ranges (or factory preset based on metrical data collected before production) This interface can be manually controlled, or left to operate automatically with no operator present. Each installed hardware 'module' throughout the designated area work independently and as a group to accomplish a number of goals for communication control.



Communication Detection & Jamming Configurations:

The telemetry is built to detect and jam some or all transmissions based upon a proprietary user defined relationship database. Detection: Detection involves a) an alert to an unauthorized incoming or outgoing cellular or WiFi data signal. b) Location of that signal on a map of the room the system is deployed in. In this sense, the system will recognize the type of signals at the point of detection as well as the Cellular Phone handset's location.



Legend:

1. Integrated Detector Jammer Hardware
2. Ground based discreet housing in Stanchions
3. Ceiling based discreet housing in Ceiling Mirrors
4. Ceiling based overt housing in dome-like security housings

Telemetry can be customized to meet the requirements of each individual installation.

Q: What does ***detect and jam some or all transmissions*** mean?
A: The user can permit a given set of communication wavelengths, such as satellite communications, yet simultaneously jam privacy-leaking non-essential frequency ranges (such as WiFi, CDMA, or GSM frequencies).

User Selectable Jamming: Because the Detector Jammer can identify frequency ranges, it can differentiate which signals to jam. For example, the jamming of cell phone frequencies of GSM 900MHz and 1.8GHz bands in Europe and the 1.9GHz and 850MHz bands in the US can be achieved while simultaneously permitting emergency communications on Satellite Phone frequencies such as:

Globalstar Sat Phone Transmit range: 1610.73 to 1620.57 MHz
Globalstar Sat Phone Receive range: 2484.39 to 2499.15 MHz
This is not a loophole but an Emergency protocol — a feature that lets the operator enact or prevent total communication silence.
Cellular Detection can be visible by:

- frequency identification
- signal strength
- graphic identifier on a map of the physical room (bird's eye 2 Dimensional mapping) [view from the ceiling to the floor level within each room of deployment]

Interference Ranges:

The Detector Jammer can let the user control the power output of RF Jamming at any of the deployed hardware installations.

That means that if there are 4 walls in a room, and the user wishes to reduce the jamming emissions of the Detector Jammer hardware close to the walls, but not in the middle of the room, the system will be able to manually reduce the jamming power output at those particular locations chosen by the operator.

RF shielding in ceiling and floor locations as well as wall perimeter points are an alternative to control jamming emission interference into adjacent rooms.

Q: Can the system enforce exact boundaries for areas of jamming and areas of non-jamming (to permit communication in designated parts of a room)?

A: Technically do so would go against the laws of physics because the jamming signal strength is dropping gradually at various boundaries based upon multiple variables.

Although there can be designated non-jammed areas, their borders would not be fixed (there could not be a permanent dividing line between the jammed and non jammed areas).

Detector Jammer Diagnostic Remote Control:

Should the administrator / operator make changes in operational configurations, there is no downtime in Detection and Jamming. The user can disable or enable a particular section or area of active signal hunting and blocking without disturbing the remnant sensor and jamming hardware.

The system is able to let the user know that a particular malfunction may have occurred and that the hardware in question has been disabled, due to possible tampering (vandalism should someone hit or break installed hardware). The rest of the system will still operate. An alert will be generated to the operator, telling which Detector Jammer module(s) have been disabled so that they can be replaced right away. Should there be a malfunction by non-external vandalism (organic internal failure) again, the rest of the hardware installations will continue to operate normally while an alert is sent to the operator indicating the problematic module.

Technical Application Data

- **Detect Cellular and 802.11 a/b/g/n Incoming and Outgoing Activity in Real Time.
If there is a Cellular Alert, the system can notify the user of an 'unauthorized' call and jam the threat. If there is a WiFi alert, the system instantly jams that threat. Cellular frequencies covered: 824-849 MHz and 1850-1910 MHz bands (Protocols of Detection Include GSM, 3G, & CDMA.) Mobile Data and WiFi PDA 'SmartPhones' are able to be detected and neutralized.**

- **Locate Active Cellular Transmission & Reception events in a Room, Rooms, or full building Configurations by displaying results mapped out on a Graphic User Interface (GUI). This GUI will indicate signal strength, the frequency of broadcast, and the location on a mapping platform.**

- **Able to engage Counter-Measures automatically in order to block active Cellular & 802.11 WiFi Communications. This feature activates the Counter-Measures in the FULL PERIMETER of the designated room. The Detector Jammer comes with Selectable Output Power (SOP). SOP enables control over RF Jamming output levels in the event the user wishes to implement RF Jamming limitations (reducing power output) on user defined modules in Real Time. This will aid in prevention of RF discharge into neighboring rooms. Although this will not guarantee Communication Free zones in the room of installation, it gives the operator the ability to attempt this.**

- **Display Cellular Location activity: The system is able to give location data of the Cell Phone users breaching communication silence. Cellular activity is displayed on one Graphic User Interface.**

- **Cellular Detection includes alarming alert data in Real Time. WiFi detection automatically triggers the RF Jamming of WiFi networks frequencies (the system is designed to operate in a WiFi Free area. . . If the Detector Jammer encounters a WiFi network, it will commence with RF Jamming).**

- **Operates on a standalone platform only.**

- **The Detector Jammer is scalable in that it can accept certain upgrades to meet the challenge of future cellular and wireless technologies. Because the system is modular, it will allow addition of new modules to focus on unforeseen threats.**

- **The Detector Jammer Can Detect Spy Phones and GSM Transmitters.**

- **RF Jamming Distance: Using ceiling and ground based hardware, the detection distance can be localized to an accuracy of approximately six feet. Using only ceiling hardware, the detection distances may decrease.**

- **For Detection: IEEE 802.3 af compatible PoE or DC local power 12-60VDC 10W will be sufficient. For Jamming: Additional power may be required.**

- **Hardware: The Detector Jammer is of modular design, with 1 module for each frequency band:
This 3 piece modular design will cover certain areas based on metric data learned via Site Survey measurements of the area marked for installation.**

Detector Jammer design origins:

The Detector Jammer was born out of the Intelligent Jamming System. The Intelligent Jamming System (or IJS) is the marriage of a Controller Area Network with ’satellite’ sensor hardware. This hardware originally tested the environment for communication activity throughout the electromagnetic spectrum. Upon discovery of active signal emanations, the system would signal an alarm and trigger a jamming signal to sever the connection between radio transmitter and radio receiver RF links.

Currently the Detector Jammer is capable of discovering and neutralizing scalable threats from (a) hidden cellular phones (b) GSM Transmitters and GSM Spy Phones (c) as well as PDA ‘SmarPhones’ exemplified in iPhone or BlackBerry dual voice & data handsets operating on GSM, CDMA, and wireless networks (3g—WiFi, etc.)

(a)

(c)

(b)

Intentional Espionage or Accidental Broadcasting?

Whether knowingly or unknowingly, a cellular mobile phone can be used to empower criminals, foreign agents, enemies of the state, and competitors with the most powerful commodity: Information. They can steal information, send information to others, as well as receive information. What kind of information? A few years ago, it was just audio voice communications. Today it may be photographic secrets, video footage, proprietary information entrusted to those in a room behind closed door meetings.

Q: How can an unintentional, random chance broadcast classified information?
A: Should a phone fall into the wrong hands, it is possible to convert into a surreptitious listening device. There are ways of installing software into certain phones in order to deactivate the ringer, to call into that particular phone, and engage the microphone. There are ways of sending commands to an iPhone and BlackBerry to conduct eavesdropping no only based on cellular frequencies, but through VOIP applications via Skype and other features that the user would not be privy to.

In essence, it could happen even without the users knowledge, so a random theft of information could happen from an un-intentional standpoint.

If information is not guarded, it can be at risk of falling into the wrong hands.