

# ARROW GSM-ED

## GSM Cellular Monitoring Systems (A5.1 Encryption) 900/1800/1900 MHz

ARROW cellular monitoring systems are U.S. export controlled and sold to U.S. Government and authorized foreign government agencies only.

### System Description

ARROW GSM-ED system is an active cellular monitoring system specifically designed to operate with an A5.1 GSM encryption. ARROW GSM-ED establishes a true "man-in-the-middle" technique whereby the ARROW system interrogates all cellular phones within range, then "locks" the targeted cellular handset to its network and acts as a clone base station.



### Applications

ARROW intercepts cellular phone calls and transmissions which can be monitored in real-time, recorded and archived for future evaluation. ARROW enables collection of audio and Short Message Service (SMS) for both forward and reverse sides of the conversation.

Through interrogation and locking of the targeted mobile, the ARROW system enables both collection and denial of service (jamming) capabilities.

### Features

The ARROW GSM-ED cellular monitoring system offers:

- Virtual Base Transceiver Station (VBTS) – 900, 1800 or 1900 MHz
- Simultaneous monitoring and recording both the forward and reverse channels of the targeted mobile handset calls
- Utilizes the technical parameters collected from the interrogating of the targeted handsets and clones itself to spoof the commercial network and act as a pass through for both mobile terminated (MT – calls to the handset) and mobile originated (MO – calls initiated by the handset).
- Available in:
  - 4-channel system: equipped to "spoof" 4 handsets simultaneously
  - 6-channel system: equipped to "spoof" 6 handsets simultaneously
- Automatically records all transmissions monitored by the system
- Computer laptop with specialized software
- Two GSM bandwidth directional 7dBm gain antennas
- Captures and archives text messaging (Short Message Service) (Capture and Interceptor Modes only)

## Specifications

- Frequency Operation Range: 900, 1800 and 1900 MHz
- Operates in:
  - fixed and mobile environments; and
  - in frequency-hopping environments

ARROW has four operational modes:

- Search of active subscriber in the nearest zone (at a distance of 1 to 600 meters from the system, 'Search Mode')
- Random Search, 'Fixed Mode'
- Search for Subscriber of Interest, 'Fixed with Target List Mode'

**Catcher Mode:** ARROW GSM-ED uses this mode as a baseline for operations. Operation is initiated by conducting a network scan to identify all commercial carriers and network parameters within range. After a network scan is completed the ARROW GSM-ED artificially creates a Base Transceiver Station (BTS) that mimics the BTS of the proximal commercial cellular network. Once this artificial BTS is created the ARROW GSM-ED transmits and attracts handsets into this cloned network. ARROW GSM-ED interrogates each mobile handset within range and displays valuable technical data to the operator. The operator can release the mobile back to the commercial network or "lock" the handset; thus, maintaining control of it.

Data collected from the handset:

- Individual Mobile Subscriber Identification (IMSI) number

**Interceptor Mode:** When operating in the 'Interceptor' mode, the system enables the following functions:

- Closed Loop Collection: When two targeted mobile phones are interrogated and locked the ARROW GSM-ED can mimic the local area cellular network – i.e. receiving incoming messages from the users registered within the internal network from one Local Area Cell (LAC).  
*Note: This mode can also be utilized to create a secure network for friendly/trusted mobiles where use of commercial networks is not available or recommended.*
- Network Spoofing: ARROW GSM-ED clones and spoofs the commercial network, thus allowing for the handsets to receive, activate and experience – interactions within the external GSM network on behalf of the registered user within the internal network.
  - This is the core system functionality enabling the "man-in-the-middle" approach to data collection
  - The ARROW monitors the paging channels of the commercial network; recognizes paging requests that are sent to mobiles within the VBTS; answers the page from the network and connects the call
  - Forces mobiles to maintain lock by utilizing a 6 minute T3212 timer for all handsets captured and locked to the VBTS
  - Surgically deny unwanted mobiles that are of no value to the operation; enabling non-targeted mobiles and friendly forces to maintain connectivity with the indigenous network

**Target Mode (Target Service):** Enables operators to gather intelligence on potential targets:

- Target Presence – a manual inquiry of a mobile handset – providing positive or negative feedback as to handset's presence in the VBTS
- Get Public Number – allows the ARROW to surreptitiously call and obtain a mobile phone's Mobile Subscribers International Dialing Number (MSIDN)

**Police Function:** ARROW-ED is able to conduct several sophisticated "hacks" on any mobile handset that is locked into the VBTS. These hacks are unrecognizable to the targeted handset and its clients:

- Hot Mic – enables the ARROW-ED operator to turn on the microphone and observe all audio voices within the phone's range. This occurs without the owner's knowledge and the phone will maintain its "standby" user interface – thereby giving no indication that an attack is occurring
- Phone Download – enables the ARROW-ED operator to download the locally stored data on the target phones. Items such as calendar, contact list, archived SMS logs, media, etc. are captured.
- Voicemail Pull – enables the ARROW-ED operator to access the network's voicemail server and receive, delete, monitor the targets voicemail; with or without a password.