Introduction:

During the last decade there has been a communications revolution with mobile telephones playing a progressively more important part. Almost everyone in the developed world has a mobile phone. Important communications are conducted via voice, text and data communications by mobile phone users in all walks of life.

Regrettably not everyone is aware of the vulnerability of mobile communications and use their mobile phones unaware that there are those who seek to benefit in a wide variety of ways by gaining unlawful access to mobile networks in order to intercept calls.

Mobile phones are vulnerable:

a) Because voice calls, SMS messages, data transmissions and all of the personal or professional information they may hold can be easily intercepted.

b) Because they can be transformed into a highly efficient ‘bugging’ device either by the user or remotely by an interested and motivated organisation.

The equipment required to conduct a mobile phone interception or surveillance is of relatively high capital value and the gains to be made through its usage would have to be worthwhile to those deploying it. However, in many cases the gains are often worth the expense and effort.

It is essential to be able to detect mobile communications interception devices and for this reason Pegasus Intelligence Ltd develops and markets mobile phone counter surveillance systems.
## Mobile Phone Surveillance:

### Active and Semi Active Surveillance equipment

Active and semi-active mobile phone and mobile network surveillance systems are of several different types:

- **a) IMSI Grabbing.** Relatively low cost equipment can be deployed to capture mobile phone identification data which in turn can be used to identify that a particular handset, belonging to a particular individual is in a locality of interest. IMSI grabbers are easily and quickly deployed and do not require highly skilled personnel to operate them. Fortunately the means by which IMSI Grabber designers exploit the mobile networks to enable handset detection leaves a tell-tale fingerprint which can be detected. Counter surveillance can be used successfully.

- **b) Active, Semi Active Interception.** Active and semi-active off-air interception systems are powerful and popular. Popular since they are able to mimic both networks and individual

- **c) Infrastructure.** There are instances of infrastructure surveillance where an entire “unofficial” network has been given over to the large scale interception of mobile communications. Whereas such a system will attempt to mimic or subvert an existing official network its characteristics can be detected.

### Counter Surveillance

The process of counter surveillance involves a survey process using equipment which is designed to detect the various signatures and fingerprints of different types and manufacture of mobile phone and mobile network surveillance equipment. Pegasus has developed both the hardware and software.

---

**Proprietary**
handsets with significant consequences. Again, the means by which interceptor designers exploit the mobile networks leave a tell-tale fingerprint which can be detected systems to conduct this activity. These systems have been programmed not only to detect different types of surveillance but also the specific characteristics of various manufacturers’ equipment.

### Pegasus NetGuard counter surveillance systems:

**Pegasus NetGuard**

With “Pegasus NetGuard” the emphasis is on high speed gathering of data in a static location or from a moving vehicle in order to quickly identify mobile network interception systems and “hacking”.

The hardware comprises a Cell Seeker III hi-speed multi network survey system fitted with multiple mobile network sampling units, a GPS receiver and roof mounted antennae all connected to a laptop via USB. Covert antennae are also available.

The laptop is loaded with Pegasus NetGuard software capable of rapid multi-network sampling of mobile network data and geo referencing for each sampling.

Its functions also include the detection and characterisation of the active and semi active mobile network and mobile phone interception systems currently available.

Geo-referenced alarms are raised on discovery and Pegasus dynamic mapping ancillary software system is also run on the same laptop providing proximity and location of interception systems.

Individual mobile phones which are the target of interception or hacking can be identified for evasive action.

**Cell Seeker III survey kit**

The features of the system are:

- Up to 8 networks are handled simultaneously
- Large geographical areas can be covered quickly or static locations scanned quickly and repetitively
- A connected laptop combines the data capture processes
- Data can be gathered at high speed (e.g. for motorway cell mapping)
- All detectable mobile network data is captured
- Extensive interceptor characterisation and detection is built in.
- Detection alarms sent via SMS or connected IT networks to monitoring central system
- Operation is heavily focussed on interception detection
- Real time dynamic mapping of interceptor location via Cell Finder ancillary software system
- Auto generation of imports for intelligence gathering back office tools
- Battery pack or vehicle power supply operation
- Covert and overt antennae options
- Active GPS on all 8 ports

The presence of a mobile network surveillance device can be quickly detected through rapid mobile network data analysis and also via characterisation of known surveillance systems. The example below shows Pegasus NetGuard in operation with a semi-active interceptor exposed during real time operation.

Example discovery of a semi-active GSM surveillance system

The location of items of interest can be automatically displayed during surveying procedures using the Cell Finder sub-system included in the Pegasus NetGuard counter surveillance package. Items of interest can be pre-loaded or added during mission execution and each can be indicated during operations by different coloured symbols on the displayed map.

An example of interception discovery and display is included below.

Active or semi-active mobile network interception systems or IMSI Grabbers can be discovered during operations as described above.
Furthermore the probable location of a surveillance system can be further refined by utilisation of the dynamic mapping included in the Pegasus NetGuard system as in the example below.

Example surveillance systems discovery during operations (Middle East)
Example location of a suspected surveillance system

**Cell Seeker Pro back office system**

Data collected from Pegasus NetGuard systems, GSM interceptors and other devices may be securely and efficiently uploaded to the Cell Seeker Pro office based system. A full suite of storage and analysis programs provide access to the following functions:

- Storage of Base Transceiver Station (BTS) data
- Storage of Cell information and BTS cross referencing
- Auto upload of survey data with creation of cell and BTS records as appropriate
- Screening and analysis of survey data
- Mapping of specific survey or mission data to provide support for surveillance
- and counter surveillance purposes enforcement evidential purposes or security mission purposes
  - Reporting
Example interception alarm