TECHNICAL CHARACTERISTICS

TYPES OF COMMUNICATIONS MONITORED

- Telephony.
- Fax.
- Data Transmission:
  - Internet (e-mail, web use, news forums, file transfers, etc.).
  - SMS.
- Three-way conversations.
- Call forwarding…

FREQUENCIES

- Frequencies of mobiles: 400, 900, 1800, 1900 MHz.
- Frequencies of microwave links.

SECURITY

- Data confidentiality.
- Secured transmissions.
- Secured work stations.

OPTIONS

- Number of subscribers monitored (from several thousand to several hundred thousand).
- Number of communications monitored simultaneously (from 30 to several hundred).
- Number of operator posts (from one to several dozen).
- Detection and identification of foreign mobile users.
- Remote operating posts.
- Detection of tapping systems being installed.
- Location on radio interface:
  - Direction finding at ground level.
  - Airborne direction finding.
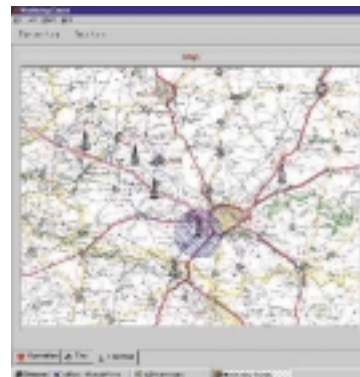- Interception over radio interface.

STANDARDS COVERED

The network solution is relatively independent from standards.

- Fixed networks:
  - Analogue.
  - Digital (ISDN…).
  - Leased lines.
- Mobile networks:
  - GSM / DCS (900, 1800, 1900).
  - GPRS, UMTS.
  - AMPS, N-AMPS, D-AMPS.
  - NMT 450, NMT 900.
  - TACS, ETACS.
  - CDMA (IS 95…).

EXPLOITATION TOOLS

- Data, text mining.
- Target networks analysis.
- Location and mapping.

THALES

THALES Communications
Information Dominance Systems
66, rue du Fossé Blanc – BP 156 - 92231 Gennevilliers Cedex - France
Tel.: +33 (0)1 46 13 20 00 - Fax: +33 (0)1 46 13 21 63
www.thales-communications.com

CELL SPYDER
MONITORING OF TELECOMMUNICATIONS NETWORKS

Cell Spyder is the result of THALES Communications' international experience over several decades, in the areas of radio and communication networks, as well as in the area of monitoring centres.
The way Cell Spyder is set up allows the surveillance of fixed and mobile networks, and also offers effective custom-made solutions for the integration in monitoring centres.
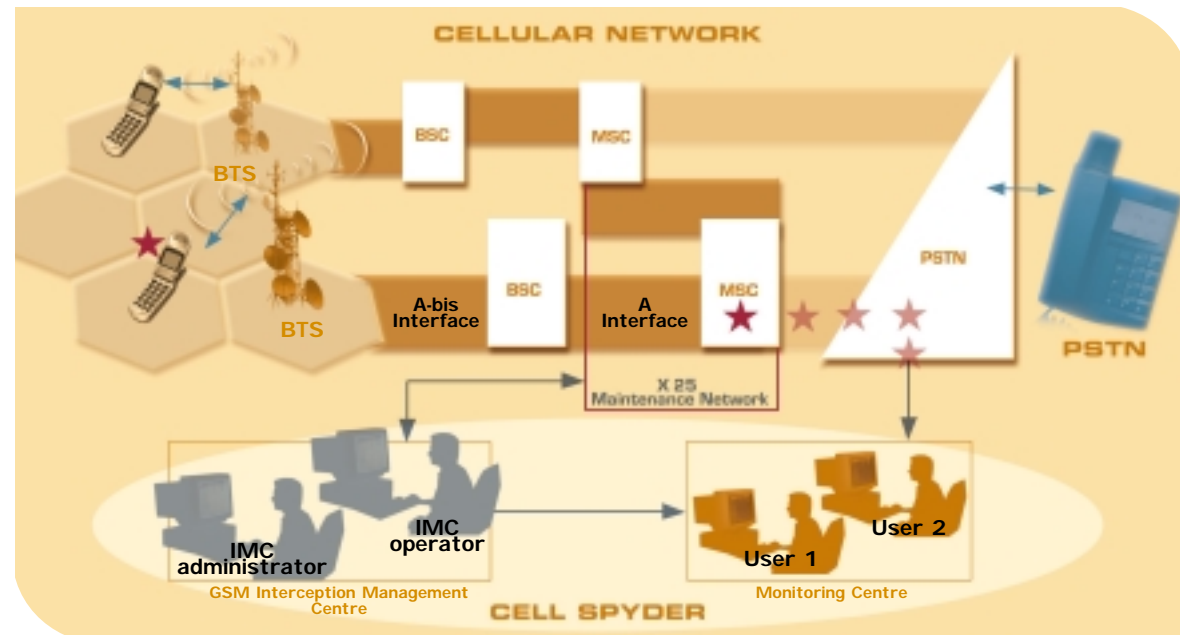
THALES

www.thales-communications.com

CELL SPYDER OFFERS GLOBAL SOLUTIONS
FOR THE CHALLENGES ENCOUNTERED IN
COMMUNICATIONS MONITORING, INDEPENDENT
ON TYPE AND SIZE OF THE NETWORK.

• Analogue or digital • Fixed or mobile • Radio interface, network interface (A, Abis)

• Multi-standard • Multi-network (future and existing networks) • Various sizes of network being monitored • Multi-manufacturer interface • Automatic digital recording

• Conforms to E.T.S.I. recommendations (ES 201 671) • Signalling (R2, N4, S5, SS7, DTMF...) • E1/T1.

CELLULAR NETWORK

BTS
BTS
BSC
MSC
A-bis Interface
A Interface
BSC
MSC
PSTN
X.25 Maintenance Network

IMC administrator
IMC operator
GSM Interception Management Centre
CELL SPYDER
User 1
User 2
Monitoring Centre

PSTN

BSC: Base Station Controller
BTS: Base Transceiver Controller
MSC: Mobile Services Switching Centre
PSTN: Public Switched Telephone Network

CELL SPYDER COMPOSITION

According to the configuration of the telephone networks to be monitored, Cell Spyder consists of:

• One or several interception management centres.

• Passive sensors (that cannot be detected by the subscribers):
  - on a cooperating network is controlled by the Cell Spyder management centre,
  - on a non-cooperating network when the network cannot "see" Cell Spyder.

• Means of routing the monitored communications from the sensors to the monitoring centre:
  - via the public network,
  - via secured networks (securised leased lines, private radio relays, etc.).

• One or several monitoring centres.

REQUIREMENTS / CELL SPYDER PROVIDES

• **Communication monitoring throughout the country**
  Cell Spyder network guarantees total monitoring of telephone systems.

• **Surveillance of a subscriber:**
  surveillance of specific subscribers through their telephone number(s).
  Cell Spyder constantly monitors every call a subscriber makes or receives. The number of target subscribers can be parameterised.

• **Communication monitoring in a specific area:**
  surveillance of all communications in the area being monitored, whether or not the subscribers have been identified previously.
  By monitoring every communication within one or several cells, *Cell Spyder tactique* makes it possible to place a specific area under surveillance, (port, airport, prison, stadium, etc.), even if the subscribers present have not been previously identified.

• **Locating service:**
  locate subscribers within the network (mobile).
  Locating is accomplished thanks to information supplied by the network (e.g. cellular networks).

• **Surveillance of a specific type of user:**
  roaming subscribers, special subscriptions...
  Cell Spyder guarantees the surveillance of a previously defined type of user (roaming subscribers, prepaid cards, etc.).

• **Surveillance of a specific type of call:**
  international calls, calls from or towards a specific country.
  Cell Spyder has the capability to filter either all international calls or calls from or towards a specific country.

• **Global surveillance of all the networks in a country:**
  allows security services to perform global surveillance, regardless of the network used.
  Today's quickly changing mobile telephony must not mask other networks. Cell Spyder manages all your pre-existing networks and offers an integrated security solution, giving to the user the ability to manage an unified monitoring centre. Centralising surveillance thus allows processing communications that come from a variety of fixed and mobile networks throughout the country (whether or not they were set up by THALES Communications).

CUSTOMERS

• **Security services.**
• **COMINT agencies.**
• **Telecom operators**, in the area of their legal responsibilities.

OPERATION MODE

• The number being monitored « blacklist » are entered at the interception management centre.

• The numbers being monitored are then sent to all the sensors by the interception management centre.

• The monitoring centre is notified each time an interception is entered or removed.

• All calls are monitored.

• Every time a monitored number calls or is called, the communication, as well as all technical information (signalling, date and time, etc.), are retransmitted by the sensor to the monitoring centre in real time.

• The communications received by the monitoring centre are then recorded in real time, and then they are either:
  - processed by operators in real time,
  - processed at a later time,
  - digitally stored for later use.