

QCC INTERSCAN

*Is your business
your business?*

Technical
Surveillance
Counter Measures





In a recent survey of American commercial organisations, 85% reported incidents of commercial espionage.

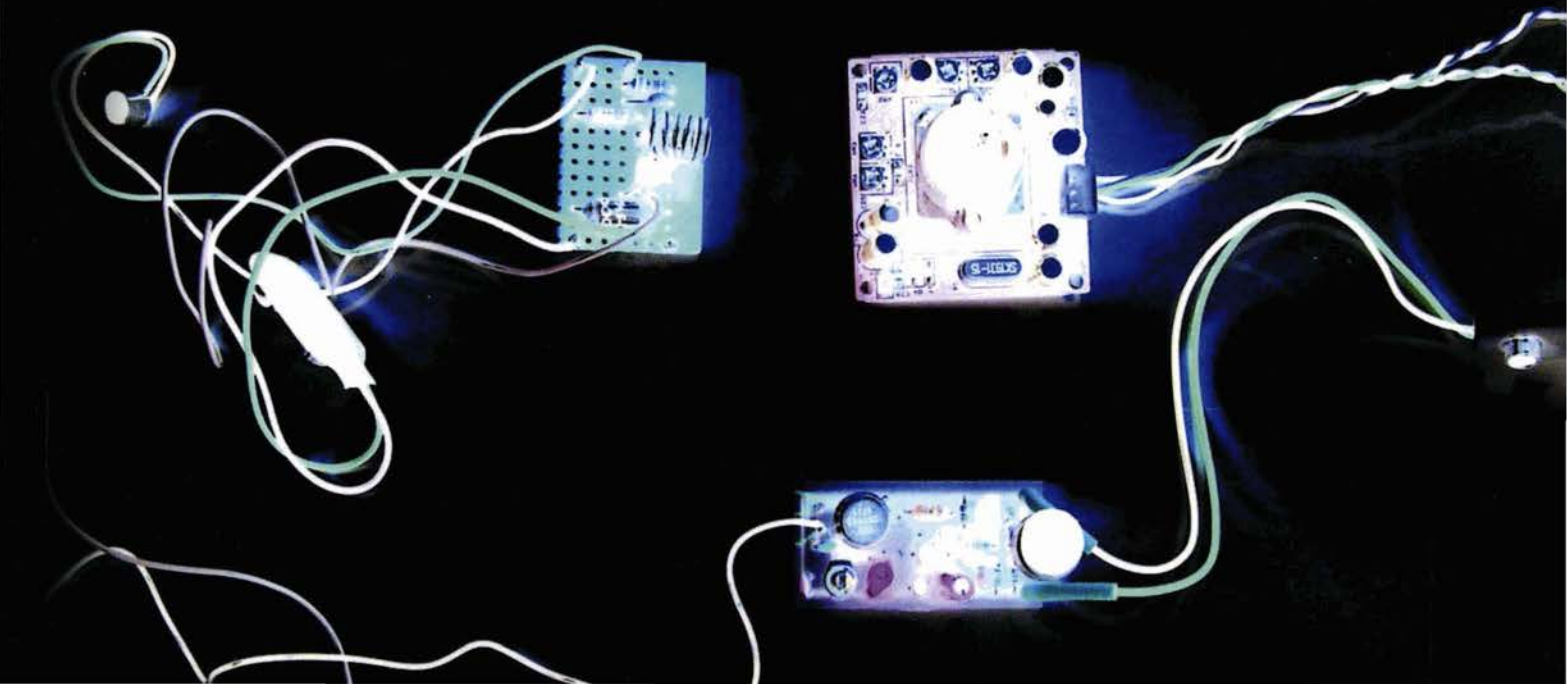
**Source ASIS
(American Society of
Industrial Security)**

How sure are you that your company's priceless business information and client confidentiality are being adequately protected?

Business is currently in the middle of an information revolution, with increasing value being placed on the sensitive data that forms the life-blood of any commercial organisation. Whether in the form of decisions taken at senior management meetings, marketing strategies, details of mergers and acquisitions, press releases, tenders or contracts planning or any other type of intellectual property, the security of this information is of paramount importance.

Quality information is expensive to acquire and therefore a potential target for theft.

Why risk transferring your company's most valuable asset to information thieves?





THE THREAT

A range of techniques may be used to steal your companies, or your clients', business information. These include radio and telephone bugging, concealed video cameras and the monitoring and hacking of computer networks and PC's. Attackers will go as far as searching through your office waste.

Deployment of concealed bugging devices takes a matter of seconds. Our experience has shown that a company's own staff is commonly used to install and move devices, often without their knowledge.

Some surveillance techniques using covertly installed software to record the victims' computer keystrokes, use email and the Internet to transmit stolen information from a victim organisation.

Your business is especially vulnerable whenever:

- Mergers or acquisitions are being discussed
- Large tenders or contracts are being invited and evaluated
- Product design and marketing strategies are being formulated
- Your service is to provide accommodation for client meetings and conferences at which confidential information is discussed
- Employees or clients are subject to the attention of the media
- Business expansion or cost-cutting/downsizing programmes are being discussed
- Work is being undertaken in a sensitive or highly confidential field
- Your company is involved in litigation

It is essential that you protect your companies, and your clients', sensitive information from this very real and tangible threat.



THE RISK

Sales of eavesdropping equipment and services are dramatically increasing. Technology has enabled a whole range of attackers to steal confidential information that may be used to their advantage, either in direct competition or to bring your company down.

These attackers include:

- Information brokers
- Private investigators
- Aggressive salesmen
- Disgruntled or disaffected staff
- Activists or terrorists
- Foreign espionage agents

The risk to your business from bugging or corporate espionage has never been greater and yet you may never realise the extent, or cause, of your loss until it is too late.

The increasing use of the Internet as a means to steal information through 'cyber spying' means that organisations are more at risk now than ever before.

By safeguarding against the threat posed by these attackers, you dramatically reduce the chances of your company becoming a statistic and increase the confidence of your staff and clients in the security of your company's future.



Searchlight GSM/UMTS detection and location system

GSM eavesdropping & tracking devices pose a threat to security !



Key features

- Easy to use
- Quick and detailed results
- Automated detection and analysis processes
- Locate and eliminate mode
- Threat analysis tool
- Comprehensive and regularly updated database

The screenshot shows the SearchLight web interface in a Windows Internet Explorer browser window. The address bar shows 'http://10.1.1.1/main'. The interface has a top navigation bar with buttons: Sweep, Admin, Print, and Off. Below this is a table with columns: Device, MNC, Connection, and Location. The table contains four rows of data, each with a 'New' button in the Connection column. At the bottom, there are buttons for Previous, Stop, and Next, and a summary section showing 'Total Devices: 4' and 'Status: Ready'.

Device	MNC	Connection	Location
1	33	New	<input type="text"/>
2	15	New	<input type="text"/>
3	10	New	<input type="text"/>
4	30	New	<input type="text"/>

Previous Stop Next

Total Devices: 4
Status: Ready

Introduction

GSM based eavesdropping and tracking devices have become by far the most common technical attack used by both commercial & government level espionage agents.

These GSM Bugging devices are available in many different hides as standard and can be purchased from the internet by anyone for as little as £ 25.00 !

They can have sound, motion & vibration activation capability & can be configured to automatically SMS the suspect or call the suspect opening up an audio channel for them to listen to the room or vehicle in question from anywhere in the world !

At QCC Interscan we pride ourselves in being world leaders in TSCM sweep service provision and in the detection of eavesdropping attacks so when the threat of GSM eavesdropping appeared we started working on a method to Detect, Locate and Counter it.

Our result is **SearchLight** !

SearchLight is the only reliable system available globally for the short range detection & Location of GSM and UMTS devices !

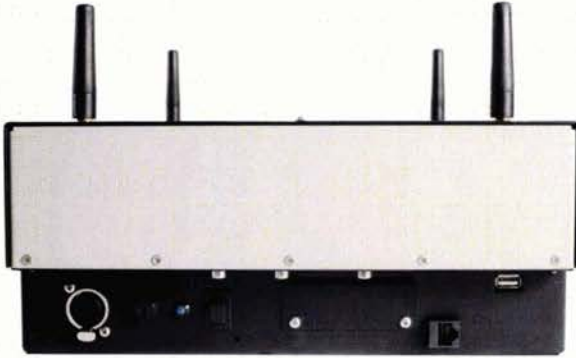
Please ask us about the many uses for **SearchLight** & how it can assist you.

SearchLight is designed & built entirely in the United Kingdom.



Searchlight GSM/UMTS detection and location system

GSM eavesdropping & tracking devices pose a threat to security !



Deployment

SearchLight is powered by a 120v -240V power supply and has a 12V input allowing it to be used in vehicles.

SearchLight also has a hold-up battery which allows the unit to be unplugged and moved from room to room without the need to power SearchLight down.

SearchLight may be deployed in a stand alone mode or in cooperative modes with other equipment or systems. Some of these deployment modes are described below.

Secure Room Systems

Users of permanent RF monitoring systems will benefit from SearchLight. These systems provide permanent and perpetual monitoring of a room or area using concealed countermeasure receivers and sensors.

These systems are locally or remotely operated and produce warning alerts when threats are detected. SearchLight adds an exceptionally cost effective capability to integrate into permanent eavesdropping detection systems.

It covers the most frequently encountered threats. Threats are constantly changing for example body worn GSM bugs may be brought into meetings. These can be detected and the operator can choose to deny service or take other appropriate action to eliminate the threat.

System overview

The system uses active, patented techniques to find any GSM and UMTS devices in the areas to be swept.

When devices are found the SearchLight operator can quickly distinguish between legitimate or authorized mobile phones and GSM bugging devices. Automated processes, network surveying, system set up and range selection, device detection and results analysis make the system effective & efficient.

SearchLight's database determines the threat level of a suspect device and is updated on a monthly basis to ensure the very latest threat information is available.

When a device is demonstrated to be hostile it can either be activated for precise location and removal or the SearchLight operator can decide to allow or deny it service at will.

White lists of mobiles can be compiled so that the system does not flag the operators mobile or other legitimate or authorised mobiles as possible hostile devices.

SearchLight is exceptionally easy to use and does not require the operator to have technical skills beyond the SearchLight training Course.

SearchLight's sweep activities and results are logged for comprehensive report generation and SearchLight can be configured to sweep networks in different Countries.

User benefits

- Easy integration into permanent RF systems
- A cost effective perpetual countermeasure
- Cost effective remote management

[illegible]

Searchlight will enable professional TSCM teams to detect hostile devices and will reduce the time required to reliably locate and eliminate them.

SearchLight can also be used very effectively to prevent VIP tracking by GPS/GSM vehicle trackers. Location and elimination of trackers is simple and efficient.

- Works along side existing TSCM equipment
- Comprehensive and current database
- Simple integration in to reports

© QCC Interscan Ltd 1998 - 2012



Searchlight GSM/UMTS detection and location system

Technical information

Uses:

SearchLight can be used to detect and locate all GSM/UMTS devices including the following kinds; Eavesdropping devices, PDA's, Mobile Phones, IED Detonation Triggers, Tracking devices, Audio and Video Codec's, Modems and Alarms.

SearchLight can be used to search People, Buildings, Vehicles, Aircraft, Watercraft and Rural and Urban Environments for GSM/UMTS devices.

Frequency bands:

The system can be supplied to cover up to two GSM bands.
All standard GSM bands are available (850, 900, 1800, 1900MHz).
UMTS bands covered include 2,100Mhz, 850Mhz and 700Mhz.

Range:

Dependant on GSM activity the range is currently between 3 Metres to 50 Metres. The range is set and adjusted by the user.

Antennas:

Omni-directional on-board antennas

Power:

12V DC Input: 4 Pin XLR Connector
Supplied with 120v-240V mains adaptor

Physical:

Dimensions: 431 x 300 x 132mm
Weight: 10kg approx
Operating temperature: 0°C to +40°C

Contact us

Address

QCC Interscan Ltd
107-111 Fleet Street
London
EC4A 2AB
United Kingdom

Phone +44 (0) 207 205 2100

Email SearchLight@qccglobal.com

Web www.qccglobal.com

*Note: This product is for use by UK Government and Government approved Agencies.
Export is subject to UK licence controls and SearchLight must be used in
accordance with local or National Laws.*

Commercial in Confidence



QCC Interscan The Global TSCM Specialists

INFORMATION PROTECTION TECHNICAL SURVEILLANCE COUNTER MEASURES (TSCM) SWEEPS

QCC Interscan is a leading Global specialist in the field of detecting sophisticated eavesdropping attacks and devices of all types whether or not they are actually operating at the time of inspection.

We use the highest quality state-of-the-art electronic search equipment to detect the presence of both active and passive surveillance devices, promiscuous monitors and keystroke Trojan horse software. We continuously monitor all emerging developments in surveillance and our equipment arsenal and methods are constantly upgraded to mitigate the risk from any new threats. Our principals are ex-Metropolitan Police Technical Support Unit engineers with over 60 years of combined counter-surveillance and information security experience.

We have extensive experience in covert technical surveillance techniques, Siege, Kidnap, telephone security and monitoring, Tracking, CCTV, Intruder alarm, Access control, Vehicle and Specialist search, and many other specialist disciplines used in the protection of important business information.

Our TSCM Consultancy services include, but are not limited to:

- Radio frequency spectrum analysis to detect illicit eavesdropping devices to 24Ghz including GSM/Digital devices
- Telephony and cable inspections to locate the presence of listening devices or modifications.
- Detection of dead or inactive electronic devices
- Full Electronic and Physical inspections
- Detection of and security testing of wireless networks
- Computer scans searching for unauthorised surveillance software's such as Keystroke loggers.
- Comprehensive physical security surveys
- IT and Physical Penetration Testing Services
- Digital forensics

Phone: +44 (0) 207 205 2100
Mobile: +44 (0) 7739 320 757
Mobile: +44 (0) 7974 242 135
Email: contact@qccglobal.com
Web: www.qccglobal.com
Ludgate House,
107-111 Fleet Street,
London.
EC4A 2AB





THE SOLUTION

QCC Interscan provides expertise in the detection of, and protection from, all forms of electronic eavesdropping. Our services considerably mitigate the risk of loss of your most important business information.

We will enable you to counter the threat of commercial espionage by protecting your most important meetings, thus providing you and your clients with the highest assurance of confidentiality.

Our specialist personnel are drawn from ex-Police operations technical support and include consultants with specialist security expertise, telecommunications and design engineering skills. All have acquired extensive technical and professional qualifications in their field.

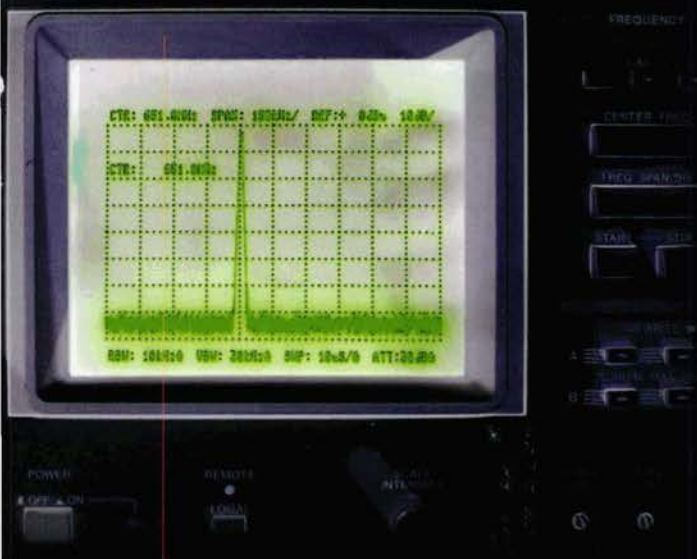
This team possesses a thorough knowledge of the traditional, modern and emerging methods employed by those who steal company information, intellectual property and other secrets.

QCC Interscan has an inventory of state-of-the-art sweep equipment. We constantly monitor new developments in the field of information security and participate in International User Groups formed to address the issues related to this subject.

Our IT security specialists scan your computer networks and systems to ensure that any attempts at 'network sniffing' or 'cyber spying' are identified and countered.

We can offer a package of technical inspections to suit your needs, including the facility to safeguard and monitor live meetings, covertly alerting you to an unauthorised surveillance attempt.

QCC Interscan has the expertise and technical capability to protect your company and clients from the damage of information theft, instilling the confidence that your business remains just that.... your business.

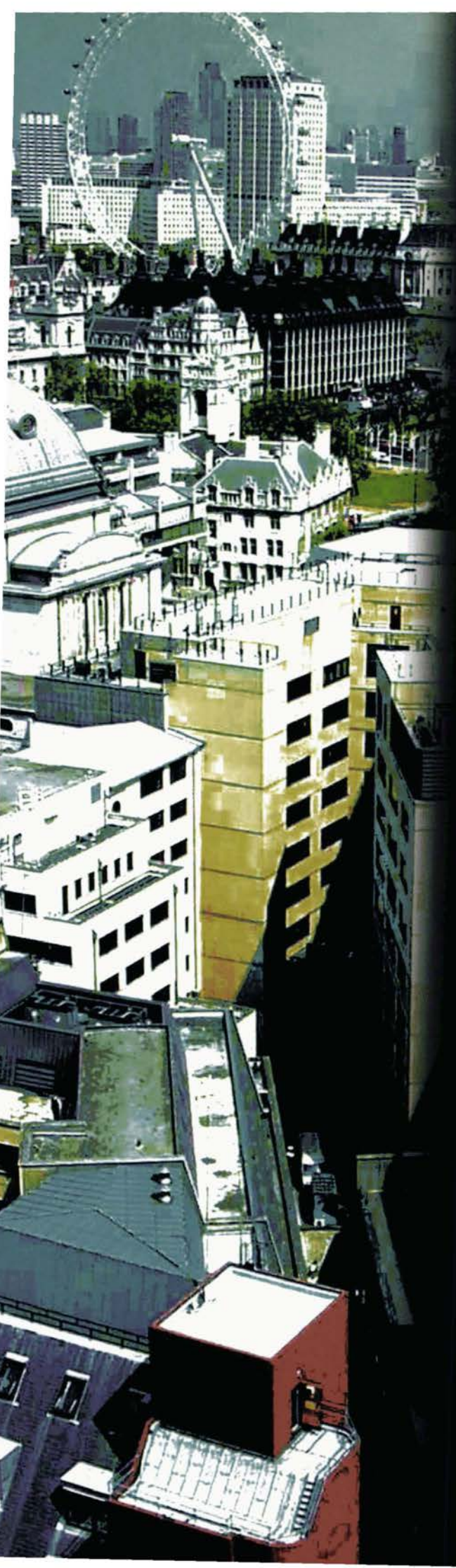


TECHNICAL SERVICE BRIEF

Our TSCM inspections include the following checks within the target area:-

- Radio frequency spectrum analysis. We check your premises for radio bugging activity using the latest RF spectrum collection and analysis equipment.
- Telephone/cabling checks. All telephone instruments and wiring, as well as electrical and all other wiring within the area, is checked for the presence of eavesdropping devices or modification.
- Non-linear junction detection test. This process uses advanced microwave technology to locate hidden or buried electronic circuitry.
- Modulated light check. We use specialist infrared detection equipment to locate eavesdropping devices that use invisible light as a means of transmitting information.
- Computer network scanning. Our IT Security experts use specialist software and hardware to detect network sniffing. Computers located in sensitive areas are analysed for unauthorised surveillance software.
- Thorough physical search. Our experts carry out a thorough physical search of the target area to detect any evidence of intrusion or modification.





QCC SERVICES

QCC Interscan provides consultancy services covering all aspects of Information Security.

Our motto Identify-Quantify-Fortify embodies our commitment to the security of our clients' business information. We pride ourselves on our ability to understand our clients' particular security requirements. From physical protection, through staff management and human resources, to complex uses of information technology, QCC provides tailored services that put the client first.

Consultancy services include, but are not limited to, the following:-

- Technical Surveillance Counter Measures (TSCM)
 - 'bug sweeping' (see Technical Service Brief)
- Risk analysis and security audits
- Emergency response to information security incidents, including investigation and forensic analysis
- Information Security policy formulation, including content security, legal and regulatory advice
- Network vulnerability testing, sometimes referred to as penetration testing (including Internet, internal networks, single host O/S and telecommunications systems)
- Implementation of security systems, including anti-virus software, firewalls, PKI, content security, VPN, Email and network encryption, laptop security and many others
- Secure systems design
- Security training and education
- Provision of specialist security software solutions



CONTACT

For further information or to arrange a consultation, please contact QCC Interscan.

Tel: +44 (0)20 7205 2100

Email: contact@qccglobal.com

Website: www.qccglobal.com

Note – Clients are advised to contact us from outside the target area.

