February 2013

intersec

The Journal of International Security

Shutting down cyber crime

How to protect your organisation

Rising terror – the threat from North Africa

As the threat from covert surveillance has grown, so too has the number of companies offering technical surveillance counter measure (TSCM) sweep services. But Gerry Hall argues equipment and experience are vital when corporate secrecy is at stake

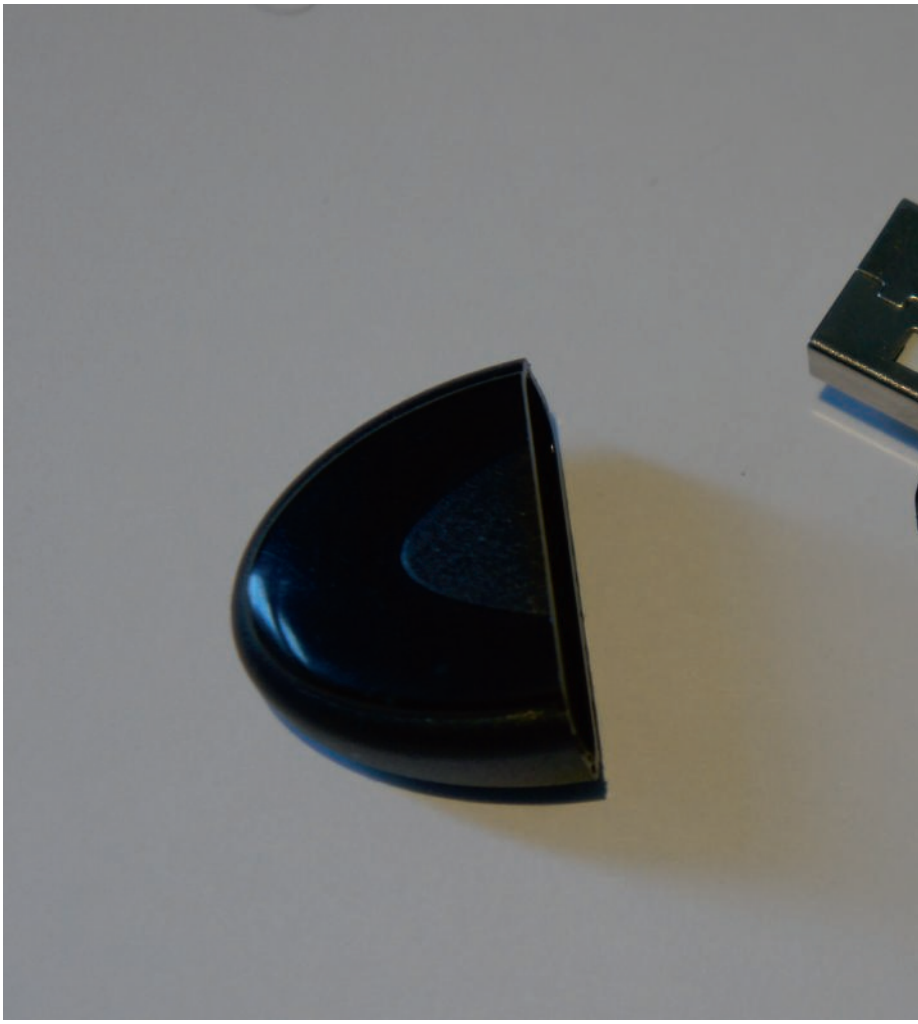
INSIDE TSCM: PART 2

PICKING YOUR

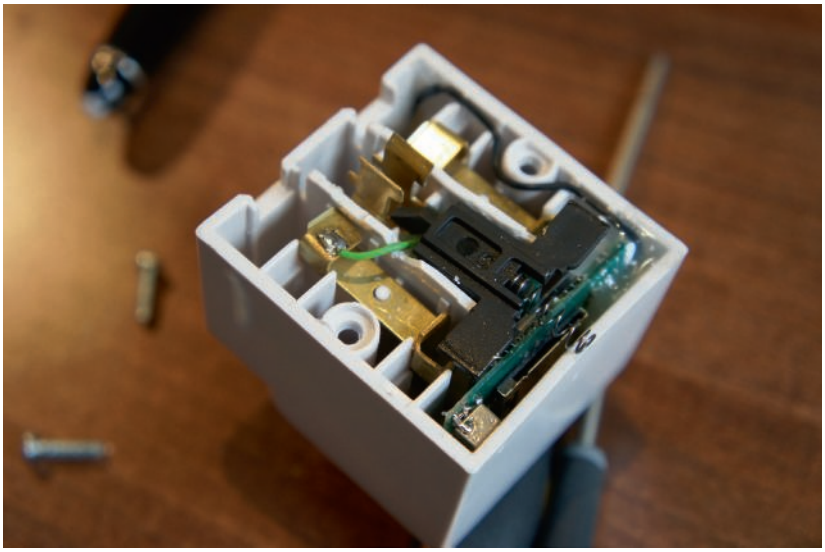
In June 2012, C. Frank Figliuzzi, Assistant Director Counterintelligence Division, FBI, told the House Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence: "In the FBI's pending case load for the current fiscal year, economic espionage losses to the American economy total more than US$13bn. The health of America's companies is vital to our economy, and our economy is a matter of national security." Well, you can be sure that the situation hasn't improved in the last seven months. Gathering information on competitors has always been considered good business practice. But there have always been those prepared to go further than simple market research and intelligence.

Industrial espionage is big business and the stakes are very high. Just one well-placed electronic listening device placed in a company board room could jeopardise a company merger or acquisition, a product launch or a share issue. Much of the problem goes unreported, as public admittance of a breach in security or loss of intellectual property, could result in even greater damage. Falling investor confidence could result in share price falls far in excess of the original losses.

In recent years the situation has become far worse with the proliferation of GSM technology. Once upon a time, eavesdropping was a specialist business requiring the perpetrator to have a high degree of skill and technological know-how. It usually meant a covert entry into the target building and the disguising of equipment that was bulky and needed a power source, and perhaps a physical line connection for long-term surveillance as well. That meant it was specialised and expensive, making it the province of only governments and the big corporations, where the stakes are highest.



©IPS



©IPS

Miniaturisation of electronics has meant listening devices have become ever smaller and cheaper. Nowadays you can buy bugs disguised as anything from a cigarette lighter to a key fob; they are encrypted, easily placed, self-powered and many can be dialled into remotely. The listener can now simply dial in using an ordinary GSM mobile phone and listen to your conversation from anywhere in the world, they can even share it via a conference call with other listeners.

Devices that ten years ago would have cost £10,000 can now be bought from the Internet for just a few pounds, and that means that everyone is

SWEEP TEAM

> **The listener can dial in using a GSM phone and listen to your conversation from anywhere in the world."**

vulnerable, from the biggest company to the smallest – from sports clubs and trade unions to individuals. The threat can come from a foreign security service, a business rival or a disgruntled employee.

It is therefore now more important than ever to have the right security policies, staff, procedures, training and equipment available to protect your business. There are a number of approaches you can take to safeguard your business or private conversations from illicit eavesdropping. One approach, as mentioned in last month's article on the subject, is a safe room. This is a selected room such as the board room, with the appropriate detection equipment permanently installed. A risk assessment may conclude that a permanent solution in a single location is not the answer for your company, however. Another route is to buy your own equipment and train your own staff in the use of the equipment. This gives you the flexibility to hold your meetings anywhere, from the board room to an office, meeting or hotel room, to a private residence.

The last option is to employ outside specialist sweep teams that come in as required – for a particular meeting, for example, or on a routine basis, perhaps twice a year – to perform a thorough sweep of key meeting rooms, offices and phones. Unfortunately, the proliferation of threats has seen a proliferation of companies offering "sweep" services. So when looking for a sweep team, it is worth using caution, because almost every private detective now likes to call themselves a sweep team specialist, and this isn't the case.

Speaking as one of the main suppliers of ECM equipment, it is fair to say there are probably only between 15 and 20 really professional teams in the UK. Each of these teams will have invested between £50,000 and £100,000 in specialist equipment. The simplest way to identify a genuine sweep team is to establish what equipment they use.

A few simple questions identify those that are able to perform the task professionally. For example, any good sweep team will always have at least one non-linear junction detector (NLJD). This piece of equipment alone will cost in the region of £11,000. An NLJD looks very much like a metal detector, but instead of detecting metal it picks up semi conductor junctions. These are used in all electronic equipment and can be detected even when the equipment is turned off or has no power. It works by radiating a signal and if there are any hidden electronics it

PICKING YOUR SWEEP TEAM

©IPS

will excite those electronics and they will re-radiate harmonic frequencies. It's these frequencies that will be detected by the equipment. Any effective sweep team will have at least one of these – either an Orion, Locator, Hawk or Broom.

Another fundamental piece of equipment is a spectrum analyser such as the Oscor Green Spectrum Analyser used by IPS or other similar devices. These are designed to scan the electromagnetic spectrum covering a broad range of frequencies. Their job is to identify any signals that are not supposed to be there, indicating the presence of some sort of listening device. Again, the names to look for are Oscor Green, Spectrum ECM, Raptor or Scanlock. Both the Oscor Green and the Raptor are from the new generation of countermeasures receivers with highly advanced capabilities regarding range and speed, allowing them to more easily identify today's complex transmitters such as burst, store and forward, frequency hopping, etc. To do this it is necessary to analyse the ambient signals in the surrounding area first, then analyse the target room; this will enable you to pick out the illicit signals from listening devices from the legitimate signals.

It is important to note these pieces of equipment are designed to be used in conjunction with one another. The NLJDs are essentially seeking non-transmitting devices such as tape recorders, remote controlled transmitters, GSM and hard wired equipment, whereas the latest spectrum analysers seek out transmitters operational at the time of the sweep.

A word about GSM detectors. Taking into account that covert GSM transmitters are the biggest threat today, it is very important to realise a detector will only detect when a cellphone is either registering or actually in use. Even then, it detects rather than locates. For example, the GSM device could be outside the building or on a different floor. Detectors are cheap, costing anywhere between £100 and £1,000 depending on quality and extra features. Very expensive equipment is available to detect and locate GSM devices, but the cost at anywhere between £30,000 and £50,000 is prohibitive, with only four or five teams having purchased such equipment.

It is also important to realise that the higher the stakes, the more sophisticated the perpetrator might be. In an attempt to avoid sweep detection, a perpetrator may use a listening device that can be activated by voice, time or a radio wave signal, such as a key fob. This may allow them to avoid detection by the spectrum analyser. Bugs may be hidden in floor or ceiling voids or in wall cavities behind plasterboard but, using a non-linear junction detector, the bug will be picked up by an experienced sweep team.

Equally important is the physical search by experienced engineers who actually know what they are looking for and, just as important, where devices are likely to be placed by a professional "buggist". Again, the GSM transmitters are really small and are being hidden in many everyday items such as memory sticks, mobile phone chargers, etc.

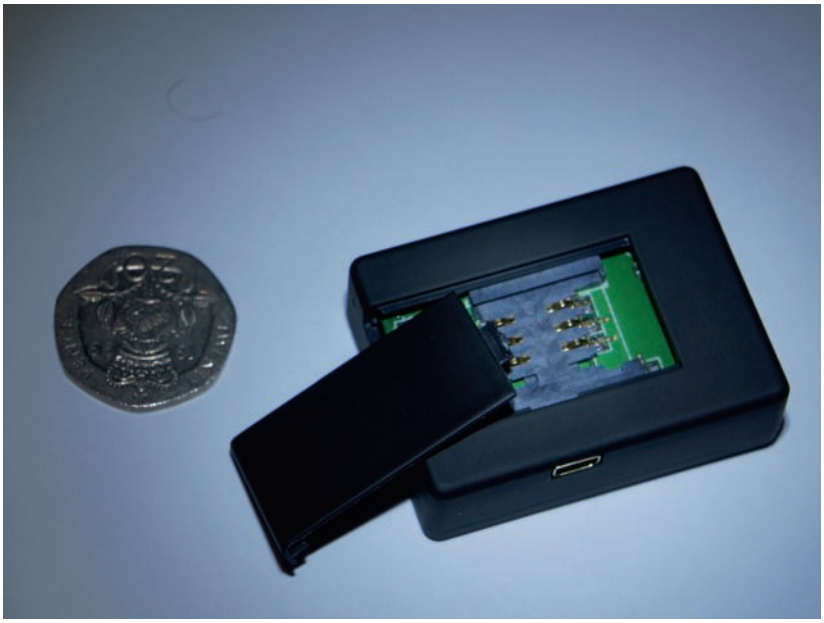
The last area of concern in any sweep is the telephone system, and for that it is necessary to use a phone and line analyser. This equipment will detect any anomalies or compromises on a phone or on the phone line, all the way back to the main switch. We use the Talan which works on analogue, digital and VoIP systems.

Your security strategies and procedures very much depend on the perceived threat, risk assessment and resources available. That the risk may change from time to time depending on your business activity is clear. But what is also clear in this growing threat environment is that having no strategy to deal with industrial espionage is no longer an option.

As a final comment, never trust a sweep company that is willing to guarantee your premises is 100 per cent "clean". It is fair to say that even the very best sweep teams would only guarantee 95 per cent security at the time they leave the premises. And then the cleaners come in unescorted…

Bugs in disguise: GSM transmitters can be hidden in a wide range of everyday objects

Gerry Hall is Managing Director of International Procurement Services (IPS) which has been in the business for more than 25 years. It has supplied this type of equipment and training to more than 100 government departments, law enforcement agencies and companies around the world.



©IPS

intersec
The Journal of International Security

ORDER YOUR SUBSCRIPTION TODAY!

intersec – The world's leading Journal of International Security is published 10 times a year. With current analytical features from a top team of contributors and in-house specialists, backed by international news pages, **intersec** is essential reading for those who take security and law enforcement seriously.

Please complete this form and return it with your remittance for the required period to the address shown below.

Subscription rates covering two and three year periods offer a valuable discount as well as enabling you to beat inevitable price rises.

2012 SUBSCRIPTION RATES

	1 Year 10 issues	2 Years 20 issues	3 Years 30 issues
UK/Europe	£125/€140	£215/€230	£280/€300
USA/Canada	US$285	US$430	US$560
Rest of World	£180	£270	£330

SUBCRIBE ONLINE: www.intersec.co.uk

Or complete and return the form below:

Please reserve **intersec** now, and send it to me at the address below for: ☐ 1 year ☐ 2 years ☐ 3 years (Please tick)

I enclose a cheque for the sum of _____ payable to "Albany Media Ltd"

Or:

Please debit my VISA / MASTERCARD / DELTA / MAESTRO

(Please delete as applicable)

Card No: ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐

(Please note that all American/Canadian card payments will be charged at the sterling equivalent)

Expiry Date: _____ ***Issue No:*** _____

Signed: _____ ***Date:*** _____

I would like to automatically renew my subscription on expiry. Please notify me and automatically debit my card unless instructed otherwise ☐

If you wish to subscribe, but your accounting systems require an invoice, please tick here, complete the rest of the form and send it to us for immediate action.

Please send me an invoice ☐

SUBSCRIBER DETAILS

Name: _____

Job Title: _____

Organisation: _____

Address: _____

_____

Country: _____ **Zip/Post Code:** _____

Email: _____

Phone: _____

If you do not wish to receive information from us in the future, please tick the boxes below:

☐ I do not wish to receive other offers from intersec (eg: our events/shows)

☐ I do not wish to receive information & special offers from other carefully selected companies

TYPE OF ORGANISATION

(Please tick a maximum of two boxes)

A1 ☐ Airline/Airport
B1 ☐ Banking/Insurance
C1 ☐ Civil Defence/Emergency Service
C2 ☐ Coastguard
C3 ☐ Customs & Excise
C4 ☐ Security Consultant
C5 ☐ Communications/Computing
C6 ☐ Close Protection
D1 ☐ Defence
D2 ☐ Diplomatic Corps
D3 ☐ Distributor/Agent
G1 ☐ Government
H1 ☐ Hospital/Laboratory
L1 ☐ Library
L2 ☐ Leisure Industry
M1 ☐ Manufacturing
O2 ☐ Offshore/Nuclear/Power
P3 ☐ Police/Law Enforcement
P4 ☐ Ports/Shipping
P5 ☐ Prison
R1 ☐ Research & Development
R2 ☐ Retail Industry
T1 ☐ Transport
T2 ☐ Training
O1 ☐ Other

PURCHASING AUTHORITY

20 ☐ Authorise
21 ☐ Specify
22 ☐ Advisory
23 ☐ Other

NUMBER OF PEOPLE IN YOUR ORGANISATION

40 ☐ 1 – 9
41 ☐ 10 – 49
42 ☐ 50 – 99
43 ☐ More than 100

Please return this completed form to:

Subscriptions, Albany Media Ltd, 22 Eastworth Road, Chertsey, KT16 8DN, United Kingdom
Tel: +44 (0)1932 566921, **Fax:** +44 (0)870 4869204, **email:** subs@intersec.co.uk. **Web:** www.intersec.co.uk

IS: