Tony Kingham on the growing importance of counter surveillance equipment and how you can ensure that your business' secrets stay safe

WHO'S LISTENING IN, A CAN DO TO STOP THE

It might be difficult to believe, but a new market for covert surveillance equipment has grown into a huge multi-million pound global business in a short few years without any governments or international authorities seemingly showing any interest in exerting any form of control.

Of course there has always been a surveillance equipment industry selling high-ticket items to governments and big organisations, but what is new is the burgeoning retail market for surveillance equipment. According to a report in the *Wall Street Journal* as far back as 2011: "A retail market for surveillance tools has sprung up from nearly zero in 2001 to about $5 billion a year".

Surveillance equipment ranges from highly sophisticated components made largely by developed nations to the newer cheaper but highly capable devices made for the retail market.

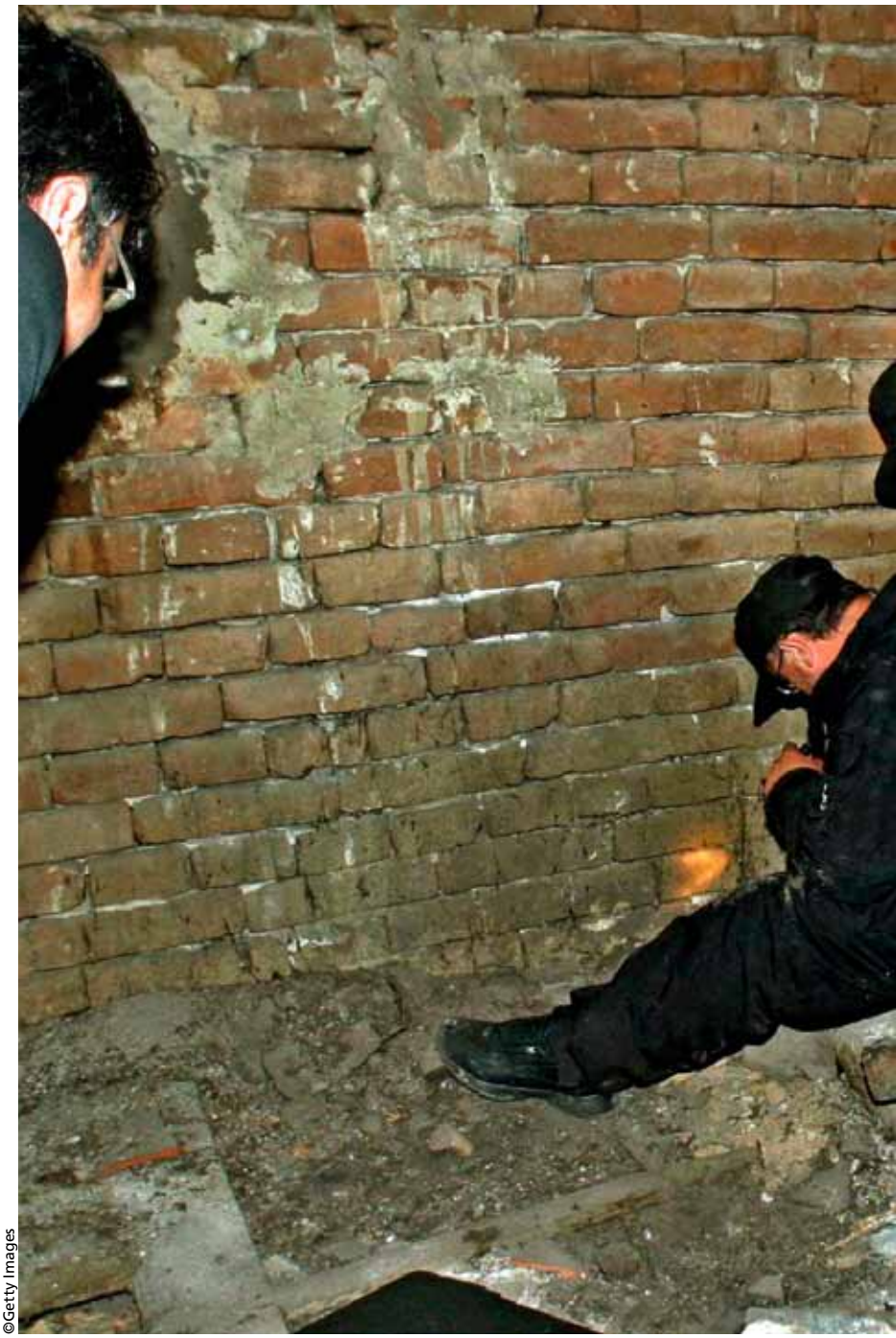
A number of factors have come together to make the new retail market possible. Miniaturisation of technologies like cameras and audio recording, the GSM system and mass production in places like China and Korea. It is now possible for anyone that has access to the web to pick up a basic listening device for a few pounds that can listen in to your conversations via the GSM system from anywhere in the world. All you need to start spying is access, a listening device and a mobile phone. So who's buying these devices and what are they using them for?

Traditionally surveillance equipment was expensive and needed highly skilled operatives to place and use, which made it the domain of governments that wished to spy on their own citizens and on those of other countries. Or big businesses that hoped to gain an illegal advantage by spying on their competitors. Of course, this market has not gone away and is still very big business for US, European and Israeli companies selling millions of dollars of equipment every year.

It is reported that former President of Panama Ricardo Martinelli paid millions of dollars to American manufacturers for surveillance equipment that he allegedly used to spy on trade union activists, politicians, lawyers, doctors and business rivals and even a bishop. Mr Martinelli is currently living in Florida and wanted on charges of corruption by the Panamanian Government.

A more recent spying scandal came to light when it was revealed that the NSA, under the orders of the White House, listened in to the conversations of Israeli Prime Minister Benjamin Netanyahu during the negotiations into a deal with Iran over its nuclear power program.

The fact that our own democratic governments are willing and able to spy on our friends as well as our enemies in a case of 'national interest' is a clue to the ambiguity that governments show towards



©Getty Images

AND WHAT YOU M

controlling the trade in espionage equipment.

After all, we expect our security services to monitor and spy on any country, organisation or individual that is deemed a threat to our security and safety. But because the security services work in a shadowy world where we the public are not privy to the information that informs on who is and who isn't a potential enemy, we have to trust the services themselves and government oversight to ensure that the right decisions are made.

In an ever-changing world this means that

Two technicians from Serbia's secret service remove listening devices from the garret above the Serbia-Montenegro Foreign Minister's party headquarters

legislating about who should and who shouldn't be spied on is enormously difficult, so by and large we rely on existing laws covering privacy and intellectual property to protect us. By the same token, it is incredibly difficult to legislate about who can and who can't buy and sell surveillance equipment.

There is an argument that the same licencing rules that apply to defence equipment should apply to espionage technology, but then you enter the very grey area of what constitutes espionage technology. For instance, when is a listening device deemed to be espionage equipment and not just a high-tech baby monitor or 'pet cam'? The same applies to micro cameras and audio recorders used for security surveillance.

Governments have tried to limit the supply of such equipment – in 2012, both the United States and the European Union imposed bans on the sale, supply, transfer and export of espionage technology to Syria and Iran. How effective this was we can only speculate, but with plenty of equipment available outside the US and EU it's anyone's guess.

Perhaps it's best to not worry too much about the high-end surveillance equipment as this remains largely the domain of governments and big corporations, but it is the superfast growing retail market in surveillance equipment that is far more likely to affect us. Why, because this technology is affordable, easily available, cheap and effective. As it so often claims in the advertising that's used to promote it: "It can make a spy of anyone".

While there is no hard data on who is buying these devices, the nature of the marketing language gives a pretty good indication.

Ebay: Do you want to know your wife/husband and friend's secret? Do you want to know what your colleagues are talking about in your office? This device allows you to spy on anyone in any place.

The sheer number of these devices available would also suggest there is a big market for them and they are in widespread use. The availability of this technology has no doubt proved irresistible to some employees that have a grievance with their boss or their company or just for the unscrupulous insider that sees an opportunity for financial gain.

Insider knowledge about companies' plans, finances, new products *etc*. can be worth millions to the right buyer, so it's not surprising that some employees will try to take advantage of this type of technology to make some serious cash.

Back in 2014 an engineer for the Ford Motor Company was dismissed and investigated by the FBI when it was alleged that she had planted eight listening devices in meeting rooms in the Ford Headquarters. This was one of those rare occasions

WHO'S LISTENING IN, AND WHAT YOU CAN DO TO STOP THEM

©Getty Images

One option is to have a safe room that you know is 'clean' from surveillance devices

when this sort of activity has come to light.

After all, the chances of being caught are slim and even if they are caught, instances of prosecution are very rare. Most companies have no desire to air their dirty laundry in public as that in itself is likely to cause them more problems and possible financial loss through dropping share prices *etc*. It is also likely to cause embarrassment and a loss faith in the management team. So most insider cases will end with an internal disciplinary action and dismissal.

Gerry Hall, Managing Director of International Procurement Services a company that specialises in anti-bugging equipment and security sweep services, notes: "Every day behind closed doors there are confidential conversations going on that can be worth multi-millions to any dishonest or disgruntled employee, business competitor, criminal organisation or foreign government. These conversations happen in offices, boardrooms, meeting rooms, hotel rooms or on the phone between business colleagues or high-value individuals. The conversation could be about a merger, product launch, buy out or share option or any number of other things that involve large amounts of money. The proliferation of GSM technology and cheap miniaturised listening devices means that everyone now has the ability to acquire technology that will allow them to listen in on conversations in any part of any building that they can gain access to, even if only for a few minutes. Via GSM they can then listen to private conversations from anywhere in the world.

"We have had 25 years' experience supplying countermeasures equipment to government and corporate offices all over the world and have performed hundreds of operational sweeps over the same period. All that experience informs us that if you need your conversations to remain confidential there is no substitute for the right equipment and the right expertise when it comes to protecting your intellectual property".

Mr Hall notes that to ensure that your conversations are not overheard, you have a limited number of options. The first is a 'safe room', which is a designated office or meeting room that has the proper detection equipment permanently installed to ensure that it is 'clean'. The second option is buying your own equipment and training your staff to use it properly. This is a more flexible approach, which allows you to use the equipment in different locations, although staff change regularly and need to stay up to date with the latest threats and techniques. This requires regular training. However, Tactical Surveillance Counter Measure equipment is expensive so for some organisations this may not be seen as cost effective.

The last option is to employ an outside specialist sweep team. The advantage of this approach is primarily experience. If you are doing something continuously, you get to know the most likely places a device is going to be concealed, as well as the more imaginative and ingenious ones. But be careful, there are plenty of companies out there that offer sweep services who don't have the right equipment to do the job. So make sure you know what they should have and don't forget to ask.

Tony Kingham is a freelance journalist and publisher of www.WorldSecurity-index.com, specialising in information and public relations within the defence and security markets. He is also Communications Director for BORDERPOL.