KCS Group Europe

The Spion Sleeps Tonight

26/02/2018

The French newspaper *La Monde* has alleged that the African Union headquarters in Addis Ababa, Ethiopia has been bugged by the Chinese since 2012. China – which also built the HQ – has of course denied such claims but this issue has raised the important point: how do you know who is really listening in?

Whether or not China is really listening to the AU, it is nothing new for one country to be listening in on another. Moscow and Washington swapped ingenious bugs during the Cold War, assorted UN and government offices are still turning up listening devices today (with the Moscow 'rock' being a particular favourite) and even during WW2 the Nazis converted the *'Salon Kitty'* nightclub into an extensive bugging suite.

The danger that concerns us today though is the high rate at which state-to-business, or business-to-business, bugging is still going on – a comparatively low-tech core wrapped up in a high-tech shell. Bugging is the third, and often forgotten, pillar of the industrial espionage doctrine. There is still nothing to beat the blackmail/coercion attempts that can be carried out by either an inside man or through judicious use of relationships, and direct hacking is similarly blunt and effective (if you know what you are looking for). But when these are not possible, or have not achieved the desired results, a traditional listening device can provide the goods – and be a lot harder to combat at the same time.

It is possible to conceal a bug in practically anything today – a pen, a plant pot, for instance, something that does not look out of place in the office environment – but for the best results one requires long-lasting battery-driven bugs that can be concealed and covered in the very fabric of the building itself, most commonly in power points or light fittings where they may not even be identifiable as alien. It would not be overly difficult to gain entry to premises, posing as electrical contractors/IT techs, for example, and use the time to judiciously secrete listening devices around key business areas that will pick up on anything said.

And the real beauty of a bug is that unless you know you are looking for it, you will almost certainly never find it. People will be naturally suspicious if one of their colleagues is constantly asking awkward questions about the top-secret projects. They will not be suspicious of talking about these projects in the privacy of an empty room.

So: something that is all-but-untraceable unless you are actively looking for it, something that puts operatives (for want of a better word) at little to no risk, and something which has the possibility to naturally pick up far more than chasing a dedicated piece of intelligence would offer. That's a win on all counts.

There are no widespread figures for how many corporates suffer bugging, but as from experience a good half-dozen companies each leading in their field have been found to have extensive covert devices around their offices (some for many years), this might be the great unknowable which in turn increases the severity of the threat. We rightly put a good deal of focus on the threats we know about – it is time we paid the same level of attention to the invisible threats which might be compromising us 24/7.

Technical counter-measure sweeps are the best way to identify bugs – and must be taken seriously with standard good practice being one every quarter – but there is also a clear need to raise awareness of what people say and where they say it, and conducting manual checks of fittings, lights, devices and so on, and taking greater note of anything new/moved/out of place - to minimise the chances of a listening device assisting its bad actors. It's arguably not paranoia – it's common sense.