



ISSUE # 8 MARCH 2010

CORPSEC QUARTERLY TSCM NEWSLETTER

IN THIS ISSUE

- ↳ WHAT IS ESPIONAGE
- ↳ INDUSTRIAL ESPIONAGE IN HISTORY
- ↳ EAVESDROPPING THREATS
- ↳ BUGGING DEVICES: KREMLIN CAT FLAP

WHAT IS ESPIONAGE



The history of espionage is quite old. The Egyptians, for example, had an extensive secret service which investigated neighboring nations as well as prominent social figures, and the Greeks and Romans also had elaborate espionage agencies. In Asia, espionage was a high art form which was exhaustively discussed in texts like *The Art of War*.

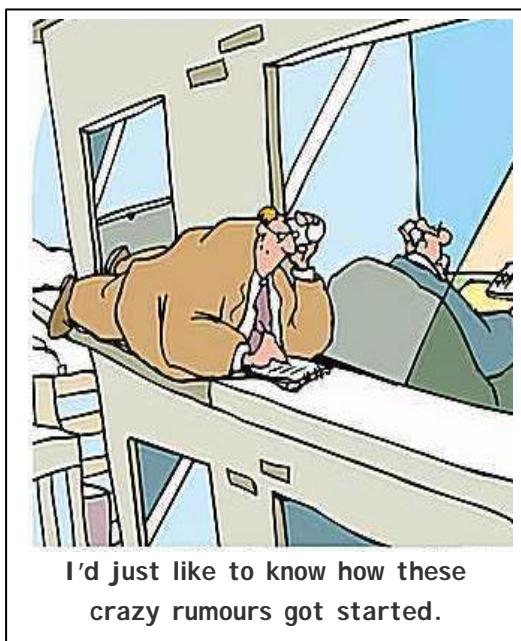
The primary distinction between espionage and other forms of intelligence gathering is that espionage involves actually accessing a site where information is held. There are a number of ways to accomplish this goal, from gaining employment as a legitimate member of an organization to breaking into a facility to steal information. In all cases, the spy must be able to quickly discern which information will be most relevant, and he or she needs tools to record and transmit the information.

Infiltration of organisations is one popular form of espionage, since it ensures a steady flow of information. For the person doing the infiltrating, of course, this form of espionage can be very dangerous, but the reward is viewed to be worth the risks.

Since espionage involves the removal of confidential and sensitive information, it is, by nature, clandestine. Many governments inform their espionage agents that they are on their own once they manage to enter a facility with restricted information, and agents are given extensive training which allows them to move quickly and ideally without detection to get the information they need. Espionage agents are also expected to conceal information about their movements, operations, and employers from other people.

EAVESDROPPING THREATS

With information becoming increasingly accessible, anyone has the potential to become a commercial spy. The Internet provides a 24-hour gateway to thousands of websites providing in-depth instructions on which listening or 'bugging' devices to purchase and effective deployment methods.



Recent quotes highlight the seriousness of the eavesdropping threat... "One London Company alone claims to have 4,500 regular customers and has taken 47,000 enquiries about listening devices within an 18 month period" SIP Services International.

"There is no challenge more ominous to global business competitiveness than economic espionage. Economic espionage is a growing threat to shareholder value with current losses estimated at \$2 billion a month." Thomas Donahue, President of the United States Chamber of Commerce.

There are an estimated 200,000 bugs and covert cameras sold in Britain every year." according to Privacy International.

The US State Department estimated in 1997 "the total annual expenditure on equipment and operations for illegal eavesdropping operations to be over \$2,213 million."

Given the sensitive subject nature and the unwillingness of victims to admit eavesdropping has taken place, the real figures are likely to be much higher.

EAVESDROPPING DEVICES - BUGS

There is no doubt that electronic listening devices, commonly known as bugs, are actively being used throughout the world.

Specialist retail outlets, mail order catalogues and Internet Websites are home to a vast number of companies selling listening devices, some costing as little as a few tens of pounds. Even the most expensive of devices can be seen as inexpensive in comparison to the value of the information sought.

With technology becoming increasingly sophisticated, microphones can be found the size of match-heads and recording devices can take shape as everyday objects such as pens and wristwatches.

Mobile phones are such a part of everyday life they are rarely given a second thought, yet they are increasingly being used as listening devices and covert cameras. Many leading suppliers offer customised services allowing customers to choose virtually any object to conceal their device.

INDUSTRIAL ESPIONAGE IN HISTORY

One of the longest lasting attempts at industrial espionage in history involved the attempt by Europeans to acquire the closely guarded secret of China's porcelain manufacturing process.

Porcelain, which had been manufactured in China since the seventh century, was brought to Europe at the end of the thirteenth century, and became greatly prized by the wealthy and elite. Due to China's monopoly on the product, porcelain was exorbitantly expensive, and Europeans tried in vain to discover the secret of its manufacture.

During the eighteenth century, a Catholic priest named d'Entrecolles was able to gain access to Kin Te-chen, the "secret city" of royal porcelain manufacturing, and sent detailed accounts of his observations to Europe. Despite tight security, he also managed to send a sample of the clay used to make porcelain, and it was not long before China lost its lucrative porcelain monopoly.



BUGGING DEVICES - KREMLIN CAT FLAP

In what was a fairly unprecedented move in spy circles, the CIA decided to implement the use of cats as a form of eavesdropping device during the height of the **Cold War** in the 1960's. According to the report in the Telegraph, the CIA believed that the cats deemed worthy of being fitted with bugging

devices, could be used to listen to secret conversations from park benches, window sills and dustbins. The crude technological ability of bugging devices at the time was not good news for the cats that were chosen for the top secret missions. Speaking to the Telegraph, former CIA officer, **Victor Marchetti**, states "They slit the cat open, put batteries in him and wired him up. The tail was used as an antenna. They made a monstrosity. They tested him and tested him. They found he would walk off the job when he got hungry, so they put another wire in to override that." So, understandably, cats weren't lining up round the block to be fitted with the bugging devices.

Unfortunately, the CIA's decision to fit cats with bugging devices was a fairly unmitigated disaster and can scarcely have got off to a worse start. The first trial run of the spy cat was a financial faux pas to say the least. Speaking to the Telegraph, Victor Marchetti stated, "They took it out to a park and put him out of the van, and a taxi comes and runs him over. There they were, sitting in the van with all those dials, and the cat was dead." Bugging devices have come a long way since the Cold War as technological capabilities have improved dramatically which, no doubt, will come as a relief to members of the feline community.



MOTHER BUGS HER FIVE-YEAR-OLD DAUGHTER'S TEDDY BEAR TO SPY ON HER EX-HUSBAND IN CUSTODY DISPUTE

By Paul Thompson

Little Bear or Big Brother?: A mother who 'bugged' her daughter's teddy bear in a bitter child custody battle is facing legal action from her ex-husband. The Mother placed a secret listening device inside her five-year-old's favourite soft toy. It allowed her to record conversations between her daughter and her estranged husband.

She hoped to use what she heard in the secret recordings in a court custody hearing. The secret recordings went on for several months. The Husband only found out he had been bugged when his ex-wife tried to use the tapes in court as evidence that he was an 'unfit' father.

But her plan backfired when a judge in Omaha, Nebraska, threw out the tapes after saying they were illegally obtained. The Judge said under Nebraska Law at least one person in the conversation has to consent to being recorded.

CAPELLO'S WORLD CUP CAMPAIGN IS NO SECRET.

The England Football Team Manager Fabio Capello was bugged while discussing his plans for this summer's World Cup Finals in South Africa. A six-hour tape of secretly recorded conversations reveals Capello's tactics for the England Squad. It is also believed to contain recordings of England players discussing financial issues.

The Football Association has launched an investigation in to how the team's security was breached. The recording were allegedly made at the The Grove Hotel in Hertfordshire, where the team were staying in the run up to a game against Egypt.

If you do not wish to receive any further Newsletters please contact Nick Graves by email.

This publication is intended only to provide a summary and general overview on matters of interest. It is not intended to be comprehensive nor does it constitute legal advice.

We attempt to ensure that its content is current but we do not guarantee its currency. You should seek legal or other professional advice before acting or relying on any of its content.



Looking after your future
Listening to your needs

Nick Graves

Phone: +61 2 9267 0661

Email: ngraves@corpsec.biz