Extracts from....
THE VMARS NEWS SHEET
A publication of the Vintage and Military Amateur Radio Society
The VMARS News Sheet Issue 128 November 2013

Operation Stopwatch – Operation Gold

The problems of EMC are only too well known to radio amateurs and have been the cause of many to abandon HF bands altogether because of the ever increasing levels of noise. It seems that even the most insignificant electrical apparatus can now be the source of very high levels of interference, sufficient to block even quite strong signals on the HF bands. Many of the unwanted emanations could be eliminated by proper design and filtering but the controls and enforcement against manufacturers who breach the standards set by the regulatory authorities are very lax. There is however, another side to these unwanted emanations, which for years have been successfully exploited for gathering secret intelligence.

I'm not sure exactly when it was realised that EMC emanations from equipment could be used to gather intelligence, but it was certainly well understood by the British at the beginning of the Cold War, shortly after the end of WWII. Like Berlin, Vienna was an occupied city, divided between the four powers of Britain, the United States, France and the Soviet Union. As depicted in the classic 1949 Carol Reed film, The Third Man, relations between the Soviets and the Allied powers were on a knife edge and Vienna was a hotbed of intrigue and mistrust. The intelligence agencies of all four countries were fighting an unseen espionage war and as a part of this the British were intercepting encrypted Soviet radio traffic. Wise to the British code breaking capabilities and having placed the free Enigma machines kindly donated to them at the end of the war onto the scrap heap, the Russian security service developed advanced encryption techniques which the Allied Powers had great difficulty in breaking. Everyone knew that telephone lines could very easily be compromised, so the focus of attention was to ensure that all data sent down these lines was highly encrypted, making it very difficult to access. However, the British knew that the acoustic, mechanical and electrical energy generated by teleprinters, encryption terminals, typewriters and similar equipment could be picked up by adjacent equipment and unintentionally transmitted down any cables connected to the building. The raw information could then be successfully compromised to extract data being processed before it had been encrypted. This knowledge, highly classified at the time, was the basis of an audacious British plan to mount an intelligence attack on Soviet land lines in Vienna in 1948.

Pre-war, the Austrians had been meticulous in mapping their underground communications lines around Vienna and these were used to identify key points for interception. The centre of Vienna was administered jointly by the four occupying powers and it was a simple matter to create a monitoring station situated close to important Russian buildings under the very British guise of a shop selling Harris Tweed clothes. Tunnels were dug from the shop to intercept communications cables servicing the buildings and EMC detectors clamped onto them. At that time, a Russian teletype, encryption encoding or similar electro-mechanical machine placed near a telephone or close to other communications or power supply lines, sent unintentional raw unencrypted data signals which were then successfully intercepted and processed. It would appear that the Russians were completely unaware of the risks of operating equipment in unscreened or electrically isolated locations and this weakness was fully exploited by the British.

The compromising emanations, or CE in intelligence jargon, are known under the codename TEMPEST and this term, along with its meaning, remained classified until the 1980's. Although computer hacking gets all the publicity these days, it generally has the disadvantage to the attacker of being detectable, whereas a passive TEMPEST attack is impossible to detect unless the monitoring station is compromised, which in the case of monitoring over a telephone line could be anywhere in the world. The risks of TEMPEST attack remain significant even now, although these days computer and encryption equipment processing sensitive and classified data is TEMPEST protected using Farady cage screened rooms and techniques such as optical isolating and filtering. A large organisation within GCHQ at Cheltenham is CESG, the Communications & Electronic Security Group, which advises military and government departments on TEMPEST protection and undertakes the management of test programmes for equipment designed and certified to meet the EMC standards that are required in sensitive areas. It's not unreasonable to assume that this group also has a TEMPEST attack capability, but if it has, it's keeping quiet about it.

By 1952, the American CIA had learned of the British interception successes in Vienna and proposed a similar joint venture in Berlin, which they designated as Operation Gold and which the British called Operation Stopwatch.

This involved digging a 10ft wide 1476ft long tunnel from the American Sector into the Russian Sector in complete secrecy and installing a monitoring post inside the tunnel under the surface cover of an American radar station. The target was a critical small group of telephone cables known to serve sensitive operational areas of the Soviet military headquarters inside the Russian Sector. The cables were located little more than 3ft below the surface and accessed from the tunnel by a narrow vertical shaft. Sensors were clamped onto the cables and fed to a series of sensitive amplifiers providing a system capable of monitoring and processing raw EMC data inadvertently picked up by the ordinary telephone apparatus and conveniently sent down the line to the British and American monitors. The crucial aspect of this type of monitoring for the Allied Powers was that the information could be accessed in its unencrypted format and because this gave them an unprecedented source of valuable intelligence, the Americans spent over $6.5 million to ensure the success of Operation Gold. Compare this to the contemporary U2 spy plane development program, with each aircraft costing $3.6 million, and it provides a clear indication of the priority they were prepared to give to this project.

The British Vienna operations ran successfully and had remained undetected by the time the four power occupation of Austria was ended in October 1955. For Operation Gold, it was unfortunate that one of the British Intelligence specialists present at a London project briefing given by the CIA was George Blake. Blake was a naturalised British national of mixed Dutch and Egyptian parentage who later became notorious as a Soviet spy code named “Diomid”, a convicted British traitor and Wormwood Scrubs escapee. He had been captured by the North Koreans while working for MI6 at the British Embassy in Seoul when it was overrun in June 1950. During his 3 years of captivity by the North Koreans, Blake, who had already been strongly influenced at school by his cousin, an Egyptian communist party leader, became a committed Marxist. In 1953 he returned as a hero from North Korea to an unsuspecting MI6. Through Blake, the Russians were aware of Operation Gold from the beginning, but for reasons not entirely understood, failed to act for over a year. Blake was an MI6 intelligence analyst, fluent in languages, including Russian and German, and was unlikely to have known about TEMPEST or the technical details of how the data would be recovered. The Russians, also unaware of its risks, believed that Operation Gold would provide no more intelligence to the Allies than had recovered when monitoring their encrypted radio traffic. Eventually, having “accidentally” discovered the secret tunnel and inspected the installation, the Russians were horrified to realise that it was unencrypted data that was being compromised. The Russians attempted to make huge propaganda from the discovery of the tunnel but failed as the world marvelled at American CIA ingenuity. The British part in this operation was not publicly revealed or acknowledged by either side because the discovery of the tunnel was made on the day before Russian First Secretary Kruschev, who was on a State visit to Britain, was due to visit Buckingham Palace for a dinner with the Queen. Although the Americans opened the details of Operation Gold to public scrutiny in 2007, the British remain tight lipped, even after over 60 years

The compromising use of EMC enabling the TEMPEST recovery of unencrypted intelligence data remained a secret for many more years, but after the discovery of Operation Gold, the Russians were fully aware of TEMPEST and implemented security measures to protect their lines of communication and data from attack. In the 1980’s GCHQ, along with several commercial companies appointed to develop TEMPEST products, gave a presentation and demonstration to the Bank of England and a group of selected key financial businesses operating in the City. The purpose of the presentation was to highlight the significant TEMPEST risks inherent when using computer equipment. No action was taken as the risks were deemed by the City businesses to be minimal. Today, illegal TEMPEST attacks on computer networks are regularly undertaken by commercial “security” companies operating in the City for the benefit of competitors.