THE TECHNOLOGY OF SECRET INTELLIEGENCE:
HOW TECHNOLOGICAL INNOVATION HAS SHAPED THE WORLD OF INTELLIGENCE

The linking theme through this talk is innovation – how engineers have found ways to overcome problems and obstacles in the search for secret intelligence.

HUMINT

The classic humint approach is to find people in target country who have good access to info or people and have willing to talk to you.

Not much technology involved except comms with agents.

Challenge – how to communicate safely with your agent – without being detected by locals.

- Low-tech – eg dead letter box (much of what you read in spy novels is true!)
- But you may want to avoid contact and that means using technology.
- Radio is obvious possibility. But still need concealment, and that is where innovation comes in. Covert radio inside book
- Or you can try to be cleverer. Moscow rock
  - 2006
  - Russian agent would come to rock and use special device to download his report; MI6 agent would go there later and upload
  - failed because of failure to think about behaviours as well as technology – FSB spotted unusual movement patterns, as spies walked round and round one flower bed.

Bugging

Challenge – how do you get a listening device close enough to your target to hear something useful? And how do you give it power? And how do you get the results out?
If you can get the right access you might plant a microphone or drill through an adjoining wall. But that's rarely possible.

In August 1945, several weeks before the end of World War II, a delegation from the Young Pioneer organization of the Soviet Union presented a carving of the Great Seal of the United States to Ambassador Harriman, as a "gesture of friendship" to the USSR's war ally. It hung in the ambassador's Moscow residential study for seven years. In 1952 it was discovered by chance that it contained a bug.
Cunning design: no power source, simply used strong radio waves at 330Mhz. Reflected waves carried the signal straight back to the Russians.

“The Thing” as it became known consisted of a tiny capacitive membrane connected to a small quarter-wavelength antenna; it had no power supply or active electronic components. The device, a passive cavity resonator, became active only when a radio signal of the correct frequency (330Mhz) was sent to the device from an external transmitter. Sound waves (from voices inside the ambassador's office) passed through the thin wood case, striking the membrane and causing it to vibrate. The movement of the membrane varied the capacitance "seen" by the antenna, which in turn modulated the radio waves that struck and were re-transmitted by the Thing.

Inventor – Leon Theremin. Will return to Comrade Theremin and his invention later.

Photography

Challenge: how do you get to watch and record activities in territory you do not have access to?

Answer in general is – get above it. Fly over it. Challenges:

- Distance
- Threat from ground attack

Early idea – photo pigeon

The WW1 version of the answer look rather Heath-Robinson, but reflects innovative use of a new technology – aircraft.

WW1 and WW2 aerial photography were all developments of that idea. Better cameras. Better planes. Proper camera mounting inside planes. They all carried the same risk of being shot down.

Cold War: Same Challenges, but greater difficulty of flying over the USSR plus threat of surface-to-air missiles
US created a plane especially for this purpose – the U2
It flew very high, above missile and fighter range. Long flight duration.

- Minimise Weight
- Thin air requires very long wings

First flight was in 1955
24 m wing-span. Note very narrow fuselage in proportion.
Altitude 70,000 ft. = over 13 miles

Camera resolution - just under 3 feet at ground level. – lots of innovation in camera design and lens manufacture
1700 miles range – 8 hour flight.
Narrow window between stall speed and speed of sound – 5 knots

Difficult to take off and land.
Note wing wheels – they fall off on take-off to save weight
Landing. Note no wing wheels. Note cycle undercarriage – very narrow.   Used a chase car because pilot can't see ground. Very vulnerable to side winds because of large wings and low weight.

In theory the U2 flew was too high for missiles but …in 1960 – Gary Powers was shot down by a new missile type.

Link between last two stories.
In UN debate of a Soviet resolution condemning US espionage, the US Ambassador produced "The Thing" to show that USSR carried out espionage as well.

US photo satellites

Planes were now no good. Try satellites.

Challenges:
- how to get decent resolution
- how to get images back

KEYHOLE programme

First successful launch of KH1 in 1960 – year of U2 shoot-down.

- Altitude 100 to 200 miles.
- Camera 24-inch (610mm) focal length.
- special 70mm high-resolution film.
- Initial image resolution 25-40 ft; a far cry from what would be standard in only a few years. It did yield, however, more images of the Soviet Union in its single day of operation than did the entire U-2 program.

KH series of satellites got ever bigger and more sophisticated.

Challenge was film retrieval. Solution was dropping film canister by parachute and having special aircraft flying in exactly the right place to catch it.

Within few years, photo resolution was 6ft – pretty good from 200 miles away. Not nearly as good as today, but good enough for experts to learn a lot.

Sigint.

Challenges:

- How to get the traffic
- How to decipher it

I'll come back to the problem of getting access to the communications later. Let me talk first about ciphers and cryptanalysis.

Cryptanalysis – code-breaking – is the clearest example of an arms race in action. People communicating want to keep their messages secret. They turn to cipher designers for systems that will help them achieve that. Their opponents want to read the secret messages: that is the job of their cryptanalysts. As cryptanalysts get cleverer, the cipher designers make their ciphers harder. So the cryptanalysts get cleverer still, and so it goes on.

Modern ciphers systems use extremely complex maths to achieve their ends. Modern cryptanalysis is all about very powerful computers and mathematics that is beyond the reach most of us, including me. There is a huge amount of innovation on both sides, but as it is both highly classified and incomprehensible, it doesn't make great lecture material. So I am going to go back to WW2 and GCHQ's forebears at Bletchley Park to illustrate my theme.

The German Enigma machine. The workhouse of German operational military comms. Familiar to most people these days.

- 3-wheels (later 4-wheels)
- Each wheel shuffles the alphabet; all different
- Each character goes through all wheels, then back again, and the cipher letter lights up.
- Then wheels move in irregular pattern for next character
- Several wheels to choose from, and wheels can be reconfigured
- Wheels can be set to any start position
- 6-leads/10-leads on stecker at front to shuffle again.

Result is 159 million million million daily set-ups to choose from. And then use different starting point for each message.

Reading Enigma depended on brilliant analysis to exploit weakness in machine and weaknesses in ways Germans used it. But even then, it required huge amount of brute force trial and error to whittle down possible settings. To make this feasible in anything like real time, the Bombe was designed. It is essentially a large number of Enigma machines running in parallel. Set up with what can be deduced about a particular message, then tests all possible settings, and stops when it finds one that looks feasible.

But Enigma was relatively easy compared to the machine used by German High Command including comms with Hitler himself– the Lorenz Schlusselzusatz 40. Rather than laboriously enciphering letter by letter for a morse operator, this machine enciphered a teleprinter. Instead of 3 or 4 wheels it had 10.

Reading TUNNY, as it was nicknamed, was a far more difficult proposition. In the end to do it on a substantial scale required a massive technological innovation. This was COLOSSUS – the world's first digital computer. It was designed by Tommy Flowers at the Post Office Research Station at Dollis Hill – a brilliant and inventive engineer.

This is not the place for a detailed technical exposition of COLOSSUS, so I want to focus on two striking examples of its innovation.

In those pre-transistor days, COLOSSUS relied upon thermionic valves. In the initial design there were over 1500; later models had 2500. The trouble is, these valves have rather limited lives. With as many as 1500, you can calculate that the machine would break down far too often to be any use. But Tommy Flowers realised that the reason valves died so often was the damage that was done each time they cooled and heated when turned on and off. His brilliant and in hindsight obvious solution was - don't turn the machine off. Ever. One consequence was that the COLOSSUS room became so hot that the WRENS who ran the machines used to dry their laundry there – but the machines kept working.

The second problem was more subtle. The machine needed a way to run the message through the programme repeatedly and continuously, and very fast. The message was encoded onto 5 level paper tape – (nb sprocket holes) . To achieve the necessary machine speed the tape had to be read at around 2000 characters per second, which meant it was moving at 30 mph. Unfortunately if you try that, the sprocket wheel just rips the tape to shreds. Tommy's answer was to do away with the sprocket wheel entirely and rely on friction and inertia – Start slow and gradually speed up.

But that creates a new problem: traditionally, the sprocket wheel was driven by the machine's clock pulse, which was critical to the synchronization of the electronics. Tommy's answer was to design a way of deriving the clock pulse from the tape holes as they passed the reader and thus maintain sync.

Deciphering messages is great as long you can intercept them.   Early in Cold War the UK and US found that the Soviets had moved many of their most interesting communications to landline. The challenge thus was – how to get at the landlines? To do that you have to look at where the cables are, and where you can get close enough in secret

Berlin tunnel

In the early Cold War days, one obvious place to look was Berlin. At that time   - early 1950s – it was a divided city, but without the Wall. So both UK and US had plenty of legitimate access; the Russians were there in large numbers; there was a good chance of valuable communications being around.

Challenges were SECRECY and SCALE

In 1954 a joint UK-US operation known as GOLD (or REGAL) dug a tunnel from American to Soviet sector in Berlin. 450 meters long, to intersect a cable that was only half a metre below a busy street.   3000 tons of material removed on a railway line. Tunnel reinforced by steel plates. Large investment in recording technology. Volumes required specially created transcription unit, staffed by Russian emigres.

- Three cables tapped
- 40,000 hours of telephone conversations
- 6,000,000 hours of teletype traffic
- 1,750 intelligence reports – military, political, USSR, Poland, GDR

REGAL ran for a year.   It was exposed by George Blake (Russian spy in MI6).

Another even more difficult operation was mounted a few years later. At the heart of the Cold War was the effort to sustain the submarine nuclear deterrents. There was - indeed there still is - a constant arms race between efforts to allow missile submarines to remain hidden and the development of technology to detect them. So information about the opposition's capabilities was crucial; and each side guarded its capabilities very tightly.   This was the origin of an operation known as ….

IVY BELLS

In the early 1970s the U.S. government learned of the existence of an undersea communications cable in the Sea of Okhotsk. It connected the major Soviet Pacific Fleet naval base at Petropavlovsk on the Kamchatka Peninsula to the Soviet Pacific Fleet's mainland headquarters at Vladivostok.   At the time, the Sea of Okhotsk was claimed by the Soviet Union as territorial waters, and was strictly off limits to foreign vessels.

So there were three challenges to overcome:

- getting access to the cable
- extracting and recording communications from it
- getting the intercept back to the US

….. and doing all that without being detected.

1971: USS Halibut mission to install operation. Specially modified submarine. Cover story was recovery of Soviet anti-ship missile that had crashed: most sailors did not know real mission.

Cable 400ft below surface. Cable not physically tapped – relied upon signal leakage, detector wrapped around outside. Separate recording unit, using mag tapes.

Every month thereafter divers went to change tapes.
Later operations in other places.
Lots of valuable intel. Very secret.
Operation betrayed by another American spy (in NSA) in 1980.

Sigint satellites.

Tapping cables to get access to comms is fine but has a very limited scope. The challenge for the West as the Cold War developed was this - how to find out what was going on deep inside of the Soviet Union? Huge land mass, huge range of comms – HF accessible everywhere, but real problem with shorter range signals, and microwave lines.

This challenge led to the advent of the US Sigint satellite programme. Still highly classified in detail, but enough is published to let us think about the challenges and some of the innovations to cope with them.

Let’s take for granted the enormous challenge of getting a satellite launched and into the right orbit. The heart of your challenge then is how to collect weak signals. It’s not like communications to spacecraft exploring the solar system, which use big dishes pointed straight at the spacecraft. In the Sigint world you are trying to intercept signals that are not being aimed in your direction and may not be very strong in the first place.

So your dilemma is this. You can put your satellite in a low orbit, so it is as close as possible to the target and you get a stronger signal; but then it is orbiting fast, and while it may hear lots of stuff it cannot dwell on it. And hearing just a few seconds of a conversation is not much use. Or you can go higher up, and dwell on a target for much longer, but now the signal strength is much less.

In practice, both techniques are used. Covering lots of ground (and sea) fast is ok for finding radar signals, where you don't need long collection times. Some types of satellite do this. Others use geosynchronous orbits: fly at 22000 miles where the orbit takes 24 hours and you can essentially hover over one spot.

22000 miles is a very long way. To collect the very weak signals, they need enormous antennae. This sketch from the Internet suggests that one series used 60 foot reflectors. And this sketch of a later system suggests 250 feet. You might like to think about the challenge of packing that up for launch and unfurling it in space.

Once the signals are collected there is then the immense challenge of processing them, and getting them back to earth. Lots of innovation …. Challenges of processing speed, data volumes, weight, space hardening …

Cyber

Finally, I'll turn to cyber. The Internet is the greatest opportunity that spies have ever known, but it also presents the greatest threats. It's an opportunity because of the sheer quantity of information it contains and the range of accesses it gives to potential targets. But it is a threat for exactly the same reasons. Hostile states can get access to government and commercial information. Terrorists use it for many of their activities, from propaganda to attack planning. And they have the potential to disrupt government and commercial activity. Criminals can have a field-day.

All this amounts to another huge arms race. Our foes - be they other nations, terrorists or criminals – are constantly trying to find vulnerabilities. We are constantly trying to block them. But we are also trying to find chinks in their armour, and they are trying to block us. And the vulnerabilities are shared; and the attack tools are often shared as well, as are the defence mechanisms. It amounts to the most remarkable ecosystem of predators and prey all swimming in the same pond. And it's a place for innovation on an unprecedented scale.

We could talk about crime, terrorism or people hacking for fun. But let's focus on the subject of my talk – espionage.

These are some recent stories about cyber espionage. I could have found plenty of others about cyber crime

What can spies do on the internet? There are really two type of activity:

- collecting information. Hack into databases.
- Disruption of other states' activities. Aka Cyber warfare. eg in time of tension, disrupt normal business by denial of service attack; or take out key facilities such as power supplies.

It's difficult to talk about cyber in the way I have talked about other subjects because there have been few public admissions about what is happening. So I am just going to talk briefly about one of the core techniques that is used by spies and criminals alike.

The technique known as a Trojan Horse, or Advanced Persistent Threat, involves getting a user on the system you want to attack to do something that will allow you to load a program onto his computer. That often involves a targeted email that appears to come from a familiar correspondent ("phishing"); the email contains a link that when clicked downloads the damaging program. Once the program is installed it can look for data it wants, send it back to the hacker, and also promulgate itself to other machines on the network. It can also sit quietly until you trigger it and then do damage to the system it is on, a useful technique for cyber warfare.

What of the future?

The "fly spy" may seem fanciful – but the dragonfly drone is a current prototype, designed by Adrian Thomas in Oxford, based on his work on how dragonflies fly.

Tailpiece – Leon Theremin

https://www.youtube.com/watch?v=w5qf9O6c20o

https://www.youtube.com/watch?v=K6KbEnGnymk