Bletchley Park

HOW WORLD WAR TWO CODE-BREAKING LAID THE FOUNDATIONS FOR TODAY'S CYBER WARFARE

British code-breakers gave the UK and US a vital advantage in the second world war by deciphering the enemy's secret communications with techniques that were the precursors of modern computer technologies

Bletchley, an unremarkable town north of London, was known until the 1970s mainly as a railway junction. But a book published in 1974 revealed that it had played an essential role in the second world war by intercepting and decoding secret communications between Berlin and the commanders of Germany's armed forces.

Slowly the full story began to emerge. At the start of the war, the British Government's Code and Cipher School had relocated from London to Bletchley Park, a mansion on a 21-hectare estate beside the town's railway station. There it devised code-breaking techniques that gave the allies an immense advantage in the war against Germany, supporting operations on land, at sea and in the air – especially on D-Day.

But the impact of Bletchley Park reached much further. By industrialising the code-breaking process and creating the world's first electronic computer, it heralded the birth of the information age. After the war, its alumni were involved in developing the earliest true computers through laboratory research at universities such as Manchester.

'The machines built at Bletchley Park were precursors of the computer, rather than computers themselves,' says Dr David Kenyon, the organisation's Research Historian. 'But I like to describe Bletchley Park as a computer system, in which some parts were done electro-mechanically and some by humans, in a process that took data in at one end and disgorged information at the other end.

'The people on the site were mimicking some of the components of modern computers, such as data processing, data storage and communications. Data was stored on card indexes, for example, for search and analysis using machines.

'It was not a static organisation – its technology and processes evolved at a tremendous rate. Staff numbers at Bletchley Park rose from 180 in September 1939 to almost 9,000 in January 1945. At its peak, the punch-card operators were getting through two million cards each week, searching them for repeated patterns in intercepted communications that could help decode them and link them to other messages.'

British code-breaking had effectively got going systematically in first world war, with at least one major success in the decoding of the Zimmermann telegram in January 1917. This secret diplomatic communication sent to Mexico by the German Foreign Office proposed a military alliance if the US entered the war against Germany. The proposal enraged US public opinion and generated support for entering the war in April 1917.

After the war, British code-breaking was passed to MI6, the Secret Intelligence Service, with a staff of around 70 who intercepted telegrams sent by the Bolsheviks and some other countries. They extended their activities to the Italians in the 1930s after the rise of Mussolini, and to Germany later in the decade after Hitler came to power.

Most of the early cipher systems were pen and paper based, but electro-mechanical systems began to appear after the first world war. German engineer Arthur Scherbius invented the Enigma machine which used a keyboard with several rotors to encrypt messages. The rotors continuously changed the code by rotating after each keystroke, and if the receiving machine was configured in the same way, it could decipher the message.

Scherbius hoped to sell it to banks and companies to keep telegrams confidential, but it was not a commercial success. However, the German armed forces adopted Enigma for military use in the 1930s, which prompted other countries to develop decoding capabilities. One which was successful in cracking the Enigma code was Poland, which feared a German invasion.

Assuming that a war would lead to bombing attacks on London, MI6 looked for somewhere to evacuate the Government Code and Cipher School and bought Bletchley Park, 80 kilometres north of the capital. When the war began, its staff moved there, along with people previously identified as promising code-breakers – mainly male British citizens with degrees from Oxford and Cambridge in subjects such as languages, mathematics and engineering. Later in the war after women were conscripted, many arrived at Bletchley Park and eventually made up 75 per cent of the staff.

By industrialising the code-breaking process, Bletchley Park heralded the birth of the information age

'There were 150 million million million possible key settings'

The School had acquired an Enigma machine in 1926, and had also been sent information on how to decode its messages from the Poles shortly before the war began. Meanwhile Alan Turing, a brilliant Cambridge mathematician who had already devised a 'universal computing machine', moved to Bletchley Park where he quickly invented the electro-mechanical Bombe machine which could help break Enigma much faster than its Polish equivalent.

'If the Enigma machine had been used correctly, its codes should have been virtually unbreakable,' says Dr Kenyon. 'There were 150 million million million possible key settings on the German machine. A brute force attack trying every combination would take an impossibly long time, even with a modern supercomputer.

'But British decoders identified weaknesses that came from the interaction between humans and the machine, developing methods still used today with cyber security. One was the requirement for code books so that both sender and receiver used the same settings – these could be stolen or captured. Another was the need to create additional settings to strengthen security, generated at random for each message. These could often be identified, since humans find it hard to be random (which is why they often cannot devise secure passwords).

'Turing's Bombe machine also exploited cribbing, widely used to decode older cipher systems. If you can guess the content of an encoded message, you can extract the message key and read other messages with it. Germans often used similar text in messages such as the weather forecast, which could provide the key for that network on that day.'

The Bombe was not a computer, but a single function machine which used telephone exchange technology. So was Colossus, a semi-programmable electronic machine devised by a Post Office engineer to speed up cryptoanalysis. By that time, 7,000 messages were coming in daily from intercept stations, and the emphasis was on decoding them quickly for indexing and analysis to find patterns.

When the US entered the war, close cooperation developed with the UK over code-breaking, which continued until the D-Day invasion of Normandy. A special Western Front Committee was created to collect information for the invasion, which was so successful that it had the complete order of battle for the German forces in France by 1944.

When the war ended, most of the staff were discharged from the armed services, instructed under the terms of the Official Secrets Act to

keep what they had done confidential. The Colossus machines and many documents were destroyed, to maintain secrecy about work that became important during the Cold War, which was why it took so long for Bletchley Park's role to emerge.

The Code and Cipher School continued as GCHQ, the UK Government Communications Headquarters which is now based in Cheltenham. It still works closely with the US National Security Agency on signals intelligence, monitoring communications which have grown enormously in volume and complexity. The methods used to identify transmitters and U-boats during the war can now do the same for mobile telephone SIM cards.

Bletchley Park had several uses after 1946, but was scheduled for housing development until a trust leased it to preserve its heritage. It has now been restored as a visitor attraction which attracts 250,000 visitors each year.

'What Bletchley Park achieved is hard to quantify,' says Dr Kenyon, 'but the impact on the second world war was significant. It helped win the Battle of the Atlantic by tracking down U-boats, and that made it possible for the Americans to get their weapons to the UK for D-Day. And the intelligence advantage it gave the allies for D-Day was immense, probably shortening the war.

'For the legacy afterwards, a lot of things were done here for the first time, but the secrecy meant that they had to be rediscovered in the 1970s. However, when people are looking back now at how IT works, how information is managed and how companies operate, it is clear that Bletchley Park was at the forefront of these developments.'●

At the time already Bletchley Park was at the forefront of how IT works today, how information is managed and how companies operate


230V
LTRS
MACHINE TYPEX
STORES REF No
SERIA No. 27
BID/08/2

One of the first Typex machine created in 1937, a British cipher machine