Cable snips and fake Mexican burglaries: How the WWI information battle was won

August 12 2014, by David Stupples

German soldiers man a wireless telegraph.

Military intelligence has relied on observing and reading enemy messages since the earliest times of conflict. But it was during World War I that great leaps were made in the technology needed to intercept enemy communications.

Intelligence gathering tactics developed in the Great War came to redefine how military operations played out and can even teach us about

how we communicate today.

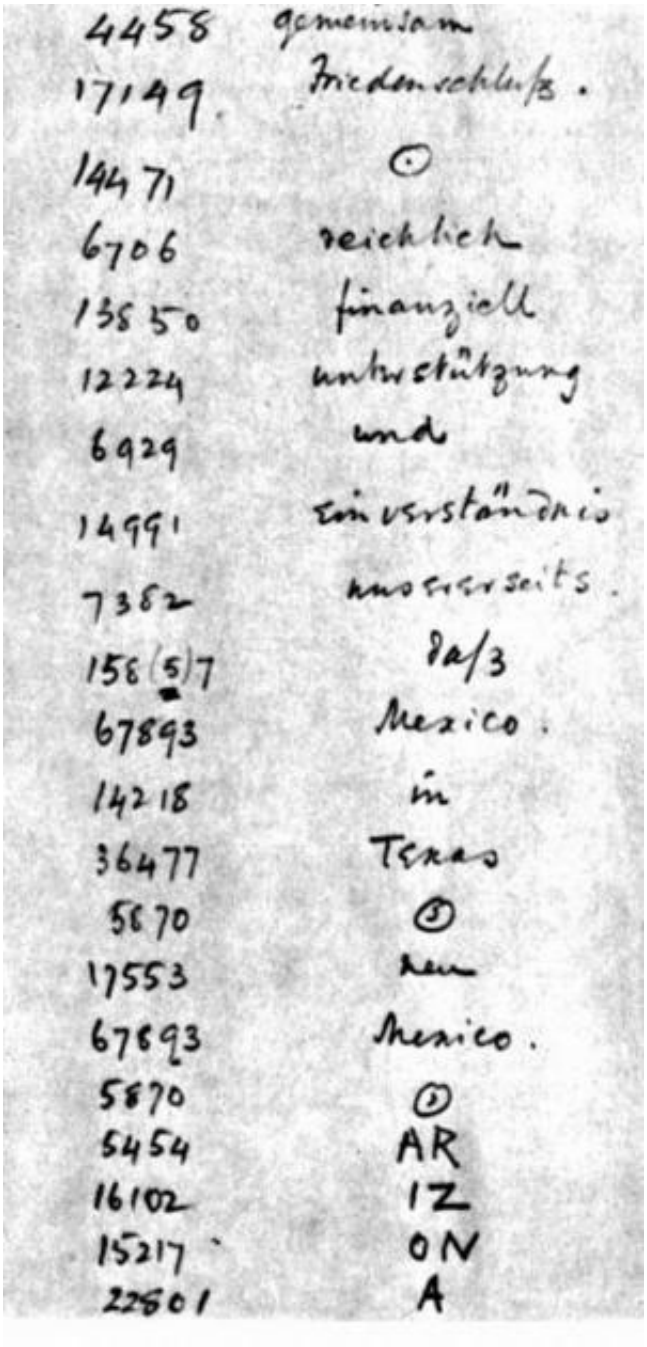
From the 15th century right up to the early 20th century, codes and ciphers were all formulated using a pen and paper. Even before then, ciphers were used in the Trojan wars. To produce them you substitute words or phrases in a message using a code book, or opt for a system like the Vigenère or Playfair ciphers which enable you to substitute a letter of pair of letters using a secret pattern.

Mary Queen of Scots and Anthony Babington used a code book to communicate details about their plan to assassinate Elizabeth I. Both the Duke of Wellington and Napoleon used code books in the Peninsular Wars and at Waterloo. Thomas Phelippes broke Babington's code for Sir Francis Walsingham, Queen Elizabeth I's spymaster, and Major Scovell broke Napoleon's code book (known as the Grand Chiffre) to influence the outcome of the Peninsular Wars.

For these systems, which are known as symmetric cyphers, the people at either end of a communication need to hold identical codebooks or pattern keys. It's a weakness that still lingers today.

Going wireless

Following the invention of wireless telegraphy, commanders began to exchange their messages in real time. But broadcasts using wireless communication could be intercepted by an enemy so it became imperative to use ciphers or encryption if secrets were to be preserved. Landline telegraphy was less of a problem if you could be sure that your enemy had no access to the landline circuit.



The decoded Zimmermann cable.

At the outbreak of World War I, the British established MI1, or British Military Intelligence, and Room 40 in the Admiralty Ripley Building in London. These organisations were responsible for communications

security, signals interception and codebreaking.

Both the French and Germans set up equivalent organisations. The French Bureau du Chiffre (Cipher Bureau) is credited with formalising codebreaking from an art into a science. The British relied more on the ability to solve puzzles, although it must be said they concentrated efforts in capturing codebooks and cipher keys to to increase their success rate. The Germans had good success with breaking Russian codes and some success with British and French codes.

Machine ciphers such as the Enigma did not appear until after World War I, so hand or manual ciphers were used in the most part. Once it became vital to communicate with troops in the trenches, a new form of encipherment was developed, called "trench codes". These again relied on code books but were designed in such a way as to be quick and easy to use as they had a limited set of two or three letter codewords that would be changed regularly.

Communications were at first based on landline telegraphy but then went wireless. To intercept wireless communications, the Germans, French and British set up dedicated wireless intercept stations which were continuously monitoring the airways. In the UK, these Y stations fed information directly back to either MI1 or Room 40 where codebreakers would get to work.

Palpable hits

A major breakthrough in the World War I battle for information came on August 26 1914 when the German Light Cruiser, Magdeburg, ran aground in the Baltic Sea off Odensholm and could not be re-floated.

The Russian Navy took advantage of thick fog and covertly boarded the vessel, retrieving two copies of the SKM (Signabuch Kaiserlichen

Marine) code book together with the usage keys. The Russians delivered one copy and key to Winston Churchill and because the Germans didn't realise they had been taken, the code book was used successfully by the British throughout the war.

Similar codebooks were also retrieved off the Australian coast from the German-Australian Steamer Hobart when the captain failed to receive information that Germany was at war.

Another major coup took place at the beginning of the war that would benefit the British for years to come. When the British Cable Ship Alert cut telegraph cables connecting Germany's link to the US, it managed to do it without Germany realising. The link had been routed via Spain and Tenerife but was redirected through the UK.

In January 1917, the German foreign minister Arthur Zimmerman sent a coded telegram via the German Embassy in Washington offering Mexico the US territories of Arizona, New Mexico, and Texas as an enticement to join Germany in a War against the US. It was intercepted at a cable connection point in Cornwall and deciphered by a team lead by Nigel de Grey in Room 40. The plain text of the telegram was passed to President Woodrow Wilson resulting in the US entering the war in Europe in April 1917. An elaborate plan involving a burglary in Mexico was hatched by the British to cover up the fact that the British had broken the German codes.

With feats like these, World War I changed the face of conflict as we know it. In 1919, Room 40 merged with MI1b to form the Government Code and Cipher School. This was later based at Bletchley Park, where codebreakers like Alan Turing went on to play a fundamental role in World War II. The operation survives to this day but is now known as the Government Communications Headquarters (GCHQ) and is based in Cheltenham.

Modern conflict management requires a constant flow of information that must remain secret if plans and operations are not to be compromised. The battle behind the scenes is between the codemakers and the codebreakers. It was ever thus from the Trojan wars to present day conflicts. But it was the Great War that first witnessed large teams of men and woman dedicated to the secret world of cryptography and cryptanalysis.

Provided by The Conversation