Electronic Warfare in WW1

by Robert Robinson

There is a common misconception that electronic warfare began with the Second World War but, even if it was not so labeled, it played a significant part in the First World War at both a strategic and a tactical level.

Both sides relied on complex cable and wireless links for communication and intelligence gathering on an international scale whilst, at the fronts, they maintained a complex web of trench and field telephone lines and exchanges. It has been said that in 1918 that there were probably more military telephones serving the Allied lines on the Western front than there were domestic 'phones in Britain, America and France. It would therefore be surprising if the Allies and the Central Powers had not attempted to damage each others networks, protect their own, gather intelligence from their opponent' networks and disseminate misleading information through it.

The Telegraph War

The electric telegraph played an important role as early as the American Civil War and by the 1870s most major armies had telegraph sections that could lay cables and relay messages. In the Franco Prussian War the French were already deploying portable telegraph sets that could be strapped to a soldier's back. The British Army in the 1880s developed a horse drawn limber system that could lay telegraph cable at the gallop. Almost all armies were still using such equipment in 1918 (although many of the cable laying vehicles were motorized).

More spectacular was the expansion of the international telegraph network, mainly through the laying of submarine cables (each cable comprising many individual wires). Every major power owned its own commercial network of cables, in time of war these came under either direct government control or close supervision. The technology had also advanced to the point where primitive forms of multiplexer and code compressors were in use to allow a single wire to handle multiple messages. Switching equipment, although fundamentally mechanical, had become complex and expensive. The destruction or damage of an international telegraph station or relay could cause considerable disruption and take a long time to replace (especially if complex equipment had to be transported to it by sea). Such stations thus became important strategic targets in time of war.

Britain with her wide spread empire and trading interests was particularly vulnerable to damage to the cable network, she was, however, well placed to protect her cables and wreak havoc on those of her enemies. Germany had a problem as, for geological reasons, most of her international cables left Europe via the English Channel. As we shall see later she made some alternative arrangements.

On August 4, 1914 Britain opened the telegraph war by cutting the German submarine cable that ran from Borkum in the North Sea to the Spanish island of Tenerife in the South Atlantic. There was a substantial German research station on the coast of Tenerife and there were fears (possibly incorrect) that this was being used as a cover for espionage and potentially for U boat support. As Tenerife lay close to the sea routes that British ships would take to Britain's West African colonies and South Africa, Winston Churchill (then 1st Lord of the Admiralty) ordered the cutting of the communications link.

The next step was the remaining German cables running through the English Channel. Many of these were simply grappled, raised and cut but some (linking to neutral countries) were patched into the British cable network this providing the Allies with additional capacity (and in the short term probably intercepting incoming messages for Germany from the remote terminus of the cable). Much of Germany's telegraph connection to the world beyond the Central Powers was destroyed.

Germany struck back, on 7th September 1914 the German cruiser SMS Nurnberg, accompanied by SMS Leipzig under cover of the French flag approached the tiny Pacific territory of Fanning Island. Fanning Island's only importance was that a submarine cable from Canada came ashore to a cable station provided the switching capacity to route messages to and from two connecting cables, one to Australia and the other to New Zealand. A landing party from the Nurnberg wrecked the station and cut the cables (they also found time to raid the local post office and steal some stamps!).

In November 1914 the crew of the German commerce raider Emden were ordered to destroy the cable station on Direction Island in the Coccos. This station provided a link between Australia and South Africa. On the morning of the 9th the cable station staff saw a warship approaching. Having been warned about SMS Emden the station's wireless operator sent out a message. "Strange warship approaching" and shortly afterwards "SOS! Emden here" before a German landing party took the station. These messages were picked up by a passing troop convoy and one of the cruisers escorting it peeled off making full speed towards Direction. The cruiser was the HMAS Sidney; within an hour and a half of battle being joined the burning Emden was beached on the nearby North Keeling Island. The landing party managed to cut one cable and wreck some instrumentation before fleeing (they made it back to Germany after 7 months via the Dutch East Indies and Turkey).

Telegraph staff under German guard Direction Island

Wireless mast destroyed by Germans Direction Island

The threat of German raiding parties was not lost on other parts of the World. In Canada, troops were despatched to guard telegraph stations on both Pacific and Atlantic coasts. In New Zealand the coastal forts, with their disappearing guns, were manned. However with the destruction of the German squadron at the battle of the Falkland Islands, the loss of the Emden and the fall of the port of Tsientao Germany had no naval force outside European waters that could threaten the international cable network.

Tapping the Telephones.

The Western Front was festooned with the wires of trench and field telephone and telegraph systems.

Field telephone exchange

Although the official British Army instruction was to bury these at least a foot and a half this was not always possible in the heat of an action. Other armies on both sides would have the same problem and wires might be laid across the open ground, draped across the tops of trenches and shell holes, lie under duck boards, be tacked along the sides of trenches or even properly buried. As the trench line altered with minor advances and retreats some wires might end up crossing from friendly trenches across no mans land through enemy positions and back to ones own side. Where enemy wires were spotted exposed in no mans, land men might crawl out at night and lay wires to tap them. In other cases shell fire or even the inadvertent clumsy boot might break the wires. In some cases, when the line was thinly manned or sentries inattentive, wire taps were even laid onto cables in the enemy's trench. The trench telephone and telegraph system on either side was not secure or reliable.

However the British began to get a sense that their calls were being intercepted with alarming ease. This was serious as the enemy might, for example, gain advance warning of a trench raid or learn when the line was thinly manned. However no one could work out why this was so. It became the common practice not to pass any important information by the trench phones but to rely on despatch riders and runners even with the risk of additional casualties to the messengers. At the same time emergency signalling methods such as warning rockets were kept handy as, with the predictably malignity of inanimate objects, the trench phone would fail just when a call for help was needed.

The cause of the security problem was found by accident when a signals instructor, Sgt Lorne Hicks, on a course in Canada found that his phone was picking up the signal of the man next to him. The British field telephone relied on a ground return system. In this the phones are connected by a single wire with the 'second wire' of the circuit being a short wire to a spike in the ground. The AC current on the phones was creating a signal through the ground that could be picked upon devices known as Moritz Stations. It was worse (easier to pick up) when the phone was being used to transmit Morse buzzes (as was the case over long lines). As the Germans perfected the sensitivity of the Moritz Stations they could 'bug' a phone from a kilometre away. Moreover, as the signal was transmitted through the ground, by creating underground saps towards the British lines they could sit at its end and pick up even more signals. One interesting sidelight to this is that the German monitors frequently picked up a whistling noise that sounded like the screech of a descending shell. Known as 'screamers' these were at one time thought to be artificial noises made by British operators attempting to 'jam' the interception; they are now known to have been created by the solar wind hitting the ionosphere – true signals from outer space.

Once the problem was identified attempts were made to find ways to intercept the German trench telephones by picking up the magnetic induction from operation of the speaker or buzzer. How successful this was is unknown as the results were classified and seem to have been lost for ever in the labyrinth of military secrecy. At the same time a British device called the Fullerphone, the invention of a Captain (later Major General) A C Fuller in 1915, was investigated and then adopted. The Fullerphone could send Morse over a 20 mile long single wire line and voice over a shorter distance. On some versions of the device it could send Morse and voice simultaneously along the same line (effectively what your broadband modem does only it's much much faster). When used on normal phone lines distance was not a problem. It used a DC signal that was much less powerful than the old trench telephone and therefore much more difficult for the Moritz Stations to pick up. At the same time the Morse system depended on a device in each phone called a 'buzz chopper', the people at each end had to synchronise their buzz choppers, these acted as a scrambling device so that no third party could listen in. As a bonus it was found that the Morse signals could be transmitted over damaged lines and across breaks (provided each side of the break was in ground contact and not too far apart).

Fullerphone in use

Like all new devices it took time to roll the new system out but it was in fairly widespread use amongst the Allies by the end of the war. More advanced versions of the Fullerphone system were in extensive use in World War Two.

Wireless Wars

In 1914 the use of wireless was largely restricted to large relatively permanent land installations and ships. The inhibiting factor was both the lack of portability of the equipment itself (particularly the receiving units) and the size of aerial needed to have any sort of effective range. By the end of 1918 wireless sets were in use in the front line, in tanks on wireless trucks, from aircraft and even motorcycle mounted.

Motorcycle mounted Marconi set

Right from the beginning wireless played an important strategic role. Germany anticipated the possible loss of its submarine cables if war broke out and invested heavily in installing powerful wireless stations in all its colonies, even the smallest. German commercial companies were ‘encouraged’ to set up subsidiaries with large transmitters and receivers in countries that were likely to be neutral. The United States was the principal country in which this was done and Telefunken established a number of stations there (they also supplied the US Army with wireless equipment).

Telefunken station on Long Island

Powerful stations were established in Germany the main one being a Nauen.. When war broke out and Germany lost its cable links it still retained a world wide network of wireless stations. Moreover by wirelessing a German station in the United States messages could then be put on an international telegraph service there. This was how many messages to and from Mexico and South America were transmitted. This was facilitated by a strange decision made by President Wilson himself, this was that, whilst to enforce US neutrality, outgoing radio messages would be subject to a Federal censor’s approval (to ensure that they were not of a military nature), there would be no control over telegraph messages carried by cable. Thus a coded message could be received by a German commercial wireless telegraphy service in the USA and then taken to an American cable service for onward transmission to anywhere in the world without any check on its contents.

Radio mast at Nauen

Britain also invested in wireless stations around the world, primarily to service the needs of the Royal Navy. These were in general not as powerful as the German stations as Britain could rely on the cable system for long range messaging. Some commercial services were also established in neutral countries, indeed the most powerful radio transmitter in the world (in 1915) was operated by the British owned American Marconi Wireless Company in the United States (after the war the US government pressurised Marconi into selling its US operation to General Electric). As one might expect the staff of the various ‘commercial’ wireless stations contained a number of intelligence officers and other forms of spook. They seem to have spent quite a bit of time trying to find ways to get around the US censors whilst at the same time monitoring the enemy’s wireless stations’ traffic so as to be able to accuse them of the same thing. Thus at one point the Marconi Company was hauled up by the US Authorities who had been tipped off that the station had transmitted a message that might help the Royal Navy intercept a German merchantman that had sailed from New York (Marconi grovelled and promised never ever to do it again, and went back and carried on as usual).

However it was British intelligence, cracking the code used for messages to and from the German station, that intercepted the German telegrams to Mexico (inviting Mexico to attack US territory) uncovered one of the issues that would bring America into the war. The same undercover activity would be found in many neutral countries. However as many of these joined the Allies in declaring war on Germany (starting with the US and Brazil in 1917) Germany’s radio network was constantly eroded.

Britain wanted the German colonial wireless stations closed. They posed a risk to British shipping as they could pass on intelligence on merchantmen's movements to German commerce raiders and at the same time help these (and blockade runners) avoid Allied warships. Some of these stations were extremely powerful. For example that in German South West Africa (today Namibia) could reach both Germany and South America. Messages could be relayed to other German colonies with lower powered stations and to commerce raiders, blockade runners and U boats in the South Atlantic and the Indian Ocean.

The very first Australian military action of World War One was the landing of a volunteer force in New Guinea to eliminate a German wireless station at Bita Paka near Rabaul. This was done, even before the Australian army could mobilise, at the urgent request of the Royal Navy. The Australians and Japanese quickly occupied those German held islands in the Pacific that housed wireless stations. Germany's wireless network had started to shrink. When Tsientao fell the German wireless net in the Far East was silenced. The stations in the German colonies in Africa took a little longer. This was in part because of a difference in priorities between France, Belgium and Britain. Many of the actions in German colonies involved cooperation between British and French or Belgian forces. Britain wished to be able to advance on and shut down the wireless stations as soon as possible whereas France and Belgium were more interested in the acquisition of territory (and to some extent taking revenge on an invader of their own countries). This sometimes created friction between the two allies, as coordinated actions needed to be negotiated. At the same time the German colonial defenders were also split between the desire to prolong resistance in the hinterland and preserve territory and Berlin's insistence that the wireless station be kept operating as long as possible.

In Togoland the German commander abandoned any thought of a prolonged guerrilla campaign in favour of protecting fortifications around the capital and the wireless station (he was still only able to hold out for four weeks but even this was deemed to by Berlin to be valuable as something like 200 messages were transmitted to German shipping enabling some valuable cargoes to evade the Allied naval blockade). In the Cameroons the local German strategy abandoned the capital and the wireless station without a fight in the face of a British amphibious operation in late September 1914 but held out in the interior until 1916. In German South West Africa wireless communications were not only maintained until the middle of 1915 but were used by the Germans to coordinate their resistance to a British/South African force attacking from the south and Portuguese intrusions in the north. German wireless stations in East Africa lasted longer although a British amphibious raid across Lake Victoria in July 21 – 23rd 1915 destroyed the transmitter and masts at Tighe.

The German station at Dar es Salaam had been destroyed by British naval gun fire in August 1914 but was rebuilt. Other stations were at Mwanza, Bukoba being able to reach the German station at Nauen, if atmospheric conditions were right. It was not until mid 1916 that the last German wireless transmitting station in Africa was silenced. Even then wireless had not ceased to play a part, the German forces, fighting a guerrilla campaign in East Africa carried with them wireless receivers that could be used to pick up messages from Germany whenever an electrical source was available and there was time to erect a temporary mast. These were in use right up to the end of the War in November 1918.

Codes, Intercepts and Deceptions

As the war continued both the Allies

and the Central Powers used wireless more and more extensively. This process was encouraged by developments in the technology that allowed wireless sets to be built smaller but be more powerful. However wireless has a serious flaw – its signals are impossible to hide. Wireless intercepts were used as early as August 1914 when German intelligence was able to listen into wireless messages being transmitted from the Russian Army HQ in Poland. Amazingly these were in clear, no attempt having been made to encrypt them (the Russian author Solzhenitsyn has said that the Russian Imperial high command somewhat naively relied on transmitting late at night when it was assumed that the Germans would have gone to bed and not be listening!). The intelligence gathered contributed to the German victory at Tannenberg.

A code system was vital to secure wireless transmission. All the major powers began to develop code systems whilst at the same time listening to each other's transmissions and attempting to break their codes. Networks of listening stations were established, perhaps the most elaborate being that established by the French under the command of a Commandant Cartier with some very tall masts (the Eiffel Tower being pressed into service to provide one of these). This allowed even relatively small transmitters in Germany to be picked up and their position triangulated and plotted. Even without breaking codes this could provide the Allies with valuable information. France created a special unit, the 8e Régiment de Transmissions, for just this work. Working under Cartier its HQ was the Eiffel Tower. Every operator tapping in Morse signals had their own style or 'fist' by which he could be 'identified' even when transmitting coded messages (although the French did experiment with a Morse key that used an oil filled relay to smooth out the operator's own rhythm). If an operator who had been previously identified as being part of the HQ of a particular military unit was detected transmitting from a new location then this would suggest that the unit had also relocated. The volume of signal traffic and any changes in this could reveal a unit held in reserve being brought up to strength and preparing for battle. The collection and analysis of such data is today referred to as ELINT (ELectronic INTelligence). As early as the beginning of 1915 Cartier could give the French High-Command a complete organisation chart of the German armies, corps and cavalry divisions.

A similar system of DF (direction finding) stations was set up round Britain in 1916 by a Capt. H. J. Round; these were used to locate German ships and proved very effective in detecting movements of the German fleet. The scope and extent of this network was kept very secret and recipients of intelligence gained as a result of its use were not told how it was obtained. Some of these stations, suitably re-equipped, were used in WW2 to pick up German signals for decoding at Bletchley Park and in the Cold War to collect data on Warsaw pact forces. They might still be in service today.

Both sides were busy trying to break their opponent's codes. The degree to which they were successful is still unclear and there are conflicting accounts. One reason for this is that if one has broken one's enemy's code it is wise to conceal the fact for as long as possible so that he continues to use it to transmit vital information. If on the other hand you become aware that your enemy has broken your code it is also a good idea to hide the fact that you know so that you can feed him misinformation. British Naval Intelligence was seeking a way to pass spurious information to the Germans and hit on the idea of devising a top secret wireless code "for the very most important messages only" and then engineering a situation whereby

German intelligence gathered enough information to allow them to break the code. A British agent travelled to Holland in the guise of an official visiting the embassy there. He stayed in a hotel known to have Dutch staff, in the employ of German intelligence, who would tip off a resident agent. The ‘official’ went out, ostensibly for a night on the town, leaving a locked attaché case in his room. This contained papers with enough information to allow an experienced code expert to create his own code book. Covert surveillance observed that the room was entered the attaché cases lock picked and a series of photographs taken. Thereafter this code could be used as a direct channel to pass misinformation mixed in with genuine but relatively harmless messages. As only British Naval Intelligence and German Intelligence had copies of the code book there was no danger of any messages being picked up by and confusing any British warships. About a year later Naval Intelligence used a double agent to sell an update of the code book to the Germans. Even to this day some histories state that German Intelligence broke the most secret British naval wireless code, which was what British Naval Intelligence had wanted people to think at the time.

There also appears to have been some use made of ‘spoof’ transmissions –wireless messages purporting to have come from friendly stations but actually sent by a hostile one. In 1917 the super Zeppelin L59 was prepared for a long range, one way, supply mission to German forces, under von Letow, still fighting in East Africa. It would carry 30,000 pounds of ammunition, weapons, medicine and bandages, materials and sewing machines for new uniforms, mail, binoculars, spare rifle bolts, spare machine gun barrels, bush knives, spare radio parts and a crate of wine. Part of the material of the outer envelope was replaced with tent fabric and considerable thought had been given to other ways in which the airship could be cannibalized to provide much needed equipment. On the 21st November 1917 L59 rose from the Bulgarian airfield of Yambol to make its long flight to the Makonde plateau. The L59 had successfully crossed the Mediterranean and Egypt and was well beyond the range of any Allied fighter bases when on the 22nd of November while passing Khartoum a wireless message ‘from Berlin’ informed its captain that the German forces in East Africa had surrendered and he should abort his mission and return to base. L59 flew back to Bulgaria covering 4,220 miles and being airborne for 95 hours. The wireless signal had not come from Berlin and von Letow was still fighting. The message had been sent from an Allied ‘spoof’ station, just one example of WW1 electronic warfare albeit a most effective one.

L59

Zeppelins raiding Britain used radio signals as a navigational aid and both British and French stations attempted to jam these by transmitting on what they assumed would be same frequencies. It was then found that the German aircrew were using the French transmissions from the Eiffel Tower to provide fixes. On the night of the 19/20th October 1917, during a major Zeppelin raid on Britain, transmissions from the Eiffel Tower were switched to another station. The effect was to give the German navigators completely false bearings. The returning Zeppelins were all badly off course, two ending up in the South of France, and five were destroyed or captured. The use of wireless to mislead was kept quiet (after all the Allies might want to do it again). The weather was bad that night with strong winds; this was given out as the reason for the disaster (and may have been a contributing factor). Even today a number of books on the Zeppelin raids fail to report the impact of wireless.

******