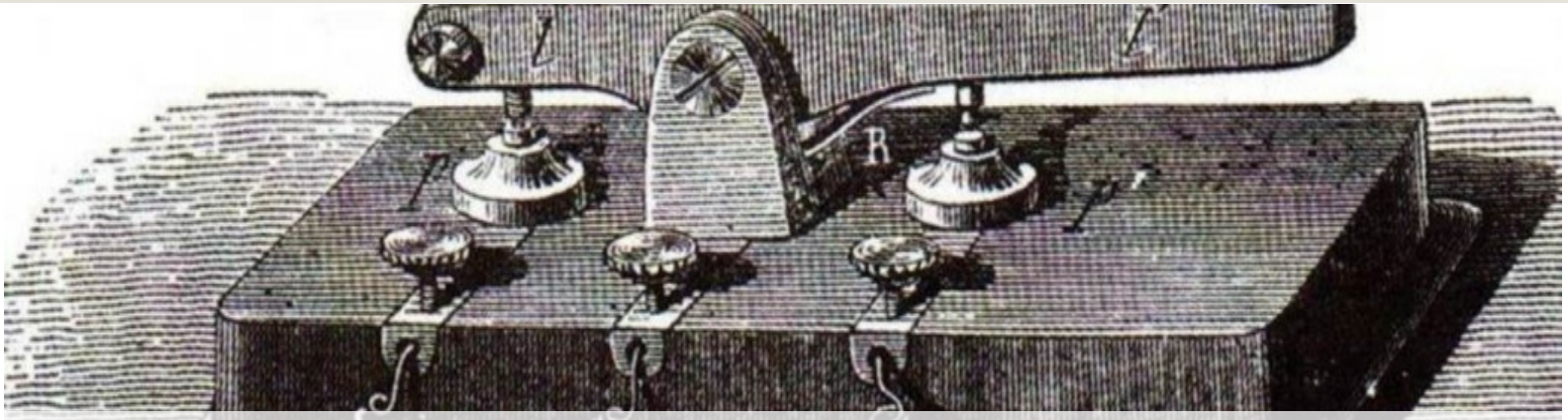

The Historical Origins of Electronic Warfare

2/2 - BRENNUS 4.0

le lieutenant colonel George Housset, du pôle études et prospective du CDEC

Published on 19/03/2020

Sciences & technologies

"Go to Rome and bring a message to Caesar. You will tell him, "All Gaul is occupied. " He will ask you: "All of it ? ». You will answer him: "All of it! "He'll understand. Goscinny

It is the fear of "interception" that is at the origin of the development of devices designed to conceal messages, whether physically (we speak of "stealth") or physically (we speak of "interception").ganography), or through the use or invention of codes and numbers, techniques used to disguise the meaning of the message so that only its intended recipient can read it (this is called cryptography).

Herodotus[31] reports in his writings the technique of tattooing the skull of messengers whose hair is left to grow back... a procedure attributed to the king of Babylon Nebuchadnezzar[32], surprising and infallible, but long! The Greek historian also tells us the story of an ancient Spartan king who took refuge with the Persian king Xerxes. When he learned of a plan to invade Greece, he decided to warn Sparta discreetly: "He took a double tablet, scraped the wax off it, wrote Xerxes' plans on the wood itself, and then covered his message with wax, so that the bearer of a blank tablet would not be in trouble. By scraping the wax, as if shaving the head, the message in clear text is transmitted. Later, sympathetic inks are used (lemon juice, milk, certain chemicals or even urine). Invisible to the naked eye, a simple flame or a bath in a chemical reagent reveals the message. Another method is to hide a message in a text. This involves imperceptibly pricking certain letters. Another method used by the Chinese is to have messengers ingest wax pellets containing instructions. In the "Gallic Wars", the great Caesar says he used this last method, which is still used in the 21st century, as are all those mentioned before.33] and which can be found in all troubled periods, from the Middle Ages to the Resistance, including the Napoleonic Wars.

The first of the codes is natural: language. It has always represented an obstacle to communication in armies using allies, whether they are Roman reinforced by the

Germans, Greek supplemented by Gauls or Napoleonic. It is in order to solve this general problem of understanding that was born on the battlefield "a language of music" (drums, brass), understandable by all. The most astonishing thing is that over time and with the development of technology, man has turned this weakness into a strength. Thus, during the Great War, the Amerindians of the American army (Choctaws and Cherokees) improved the security of communications at the front by communicating in their only native language, incomprehensible to the Germans. During the Second World War, the "Code Talkers" were the Comanches in France, the Meskwakis in North Africa and above all the Navajos in the Pacific, whose language was not written at the time and whose grammar was very complex[34]. 34] The "code" proved to be impenetrable throughout the conflict.

Who invented the first secret artificial code: the Indians, the Chinese, the Egyptians? In any case, the Greeks seem to have been the first to distinguish themselves in order to conceal their strategic correspondences. As early as the 5th century BC, the Spartans invented a so-called transposition algorithm, which consists in reversing the order of the letters according to a mechanism. They used scytate. It is a simple stick around which a leather or papyrus ribbon is wound in a spiral and on which it is sufficient to write lengthwise. Once it is removed from its support, it is impossible to reconstruct the order of the letters without a stick of the same diameter. The message is worn as a belt. One of the first encryption techniques used by the Hebrews, the Atbash, consists of a letter substitution algorithm. It involves replacing one letter of the alphabet with another in a specific order. In this case: A becomes Z, B becomes Y etc. Caesar also uses a letter substitution algorithm. In the case of "Caesar's number", each of the 26 letters is replaced by the letter that is three positions further down the alphabet. The disadvantage of this shift cipher is its lack of security, since there are only 25 possible shifts. The procedure was nevertheless used by Southern officers during the Civil War and by the Russian army in 1915. Encrypted dictionaries supplement the main military cryptographic systems, and are referred to as mono-alphabetic substitution encryption [36], which consists of replacing one letter by another, following a "table".

Soon a duel was established, which has been uninterrupted ever since, pitting the inventors of ciphers and keys against the cryptanalists, who break seals and mysteries. History teaches us that the latter are always victorious. Of course, they start from a blank sheet of paper, but they know the language of their opponent. There are only two methods of decryption: act empirically by trial and error, or logically by trying to understand the encryption algorithm, i.e. the logical order of the substitution or transposition operations that make up the encryption. We then hunt down what can be likened to "similarity" and "regularity". The spaces and frequencies between the signs allow for initial suspicions. After many failures, a letter or a word is probably discovered and then verified, and a second and third one is deduced. When the First World War broke out, the human brain seems to have reached a sort of threshold in the possibilities of encryption. Indeed, it is observed that while several new numbers appeared between 1914 and 1918, they were all variants or combinations of 19th century codes that had already been deciphered. Thus, a new code introduced by the Germans in March 1918 (the ADFGVX system), is inspired by a square of the Greek historian Polybe [37], a process that dates back to antiquity! The principle is an encryption by homophonic substitution (to avoid a frequency analysis, a letter is replaced by a symbol chosen at random among several). Lieutenant Painvin [38], who graduated as a major at the Ecole Polytechnique in 1905, deciphered it in extremis in a few days, while the Germans were a hundred kilometers from Paris, which allowed General Mangin [39] to mobilize troops placed in reserve to block and repel, at the end of a five-day battle, the last German offensive.

The Second World War put an end to manually formulated encryption/decryption. Grey matter was no longer enough, abstraction was "mechanized" and machines that think were invented to defeat machines that scramble. Enigma[40] is a mechanical encryption machine that incorporates a polyalphabetic substitution encryption method, i.e. an improved version of the "Caesar's cipher". But instead of having one letter systematically encrypted by another, the trick in the mechanics is to introduce a key that allows the letter to be camouflaged to be designated by several others at random, which complicates decryption. Nevertheless, the machine also has its weaknesses. Thus, the letter A is never coded by an A and two different letters typed in a row never give, twice in a row, the same encrypted letter... this eliminates combinations. Enigma is finally defeated by the British. They proceed by a logic based on the knowledge of the internal workings of the machine and the exploitation of the imprudence of the German ciphers (sending recurring words). The Germans also have Lorenz encryption. The latter is mainly used by senior German managers to communicate with each other. Unlike Enigma , the Lorenz machine can code each letter independently. "Electromechanical bombs," machines designed to decrypt coded messages, eventually defeat both means of encryption. At the end of the Second World War, Winston Churchill[41] wrote to the British cipher: "Never in history has so few men held the fate of so many in their hands.

Conclusion

Electronic warfare is, of course, a recent discipline that emerged a century ago. But when we wrote in 2004: "Electronic warfare, master of the airwaves, master of the world..." [42], it is only the gradation of an observation already formulated in 1992 by Army General Marc Monchal, Chief of Staff of the Army, who then declared: "in the future, the master of the electron will prevail over the master of fire"; a statement which is still valid today.These remarks are themselves similar to a 1953 statement by the engineer general Combaux who already claimed: "telecommunications have become the third fundamental element of war as important as fire and movement"[43]. 43] Thus, if the French army is today faced with a new major challenge, that of the war of cyberspace, the war of communication has always had a protean face that is not fundamentally different from the problems of the day.

Indeed, it is easy to speak today of "an enemy that would not be identified", we seem to regret yesterday's wars where "confrontation was physical" and we evoke "new threats, cyber-attacks". Historicity reminds us precisely that since antiquity, the enemy was not precisely identified and that war has always gone far beyond the perimeter of physical confrontation. As for the first cyber-attack in history, isn't it the affair of these two brothers from Bordeaux, founders of an investment company, who speculate on the stock market? Thanks to the bribery of some civil servants, in charge of communication between Paris and Bordeaux, they obtain, before their competitors, the information coming from the Paris stock exchange, which allows them to obtain juicy profits. We are not in the 20th century and in the age of the Internet, but in 1834 and the pirated means of communication is the Chappe telegraph!

This last example opens a new debate: is tomorrow's history already written?

———————

31] Herodotus (485 B.C./426 B.C.), Greek historian and geographer.

32] Nebuchadnezzar (600 BC/562 BC).

33] In 1980 a letter from a deportee was discovered, written in sympathy ink, describing the horrors of the camps.

34] The film "Windtalkers" by John Woo, 2002, pays a vibrant tribute to them. In the film, Nicolas Cage's mission is to protect "the code", represented by two Indians, and prevent them from falling into enemy hands.

35] It is stated that, based on the experience of the First World War, Adolf Hitler sent some thirty anthropologists to learn the Amerindian languages before the Second World War. The Navajo tribe is the only one not studied and its language is absolutely incomprehensible to Europeans, Asians and even other tribes. These peculiarities make it a safe natural "secret code".

36] That is, the principle of "Caesar's number".

37] Polybius (200 BC/around 118 BC).

38] Painvin Georges (1886-1980). Professor at the mining school of Saint-Etienne, then of Paris before the war, geologist and palaeontologist by training, but passionate about 'numbers', he deciphered more than 240 German messages during the conflict.

39] Mangin Charles (1866-1925).

40] The patent, which dates from 1919, was granted to Hugo Koch (Dutch). The German Arthur Scherbius created the machine.

41] Winston Churchill (1874-1965).

42] Jean-Paul Siffre, General of the Air Force, French expert in electronic warfare. His work appears in the collection "Renseignements et guerre secrète", Lavauzelle.

43] Edmond Combaux, General Engineer 1st class, "Electronics and Warfare of the Airwaves", Paris, 1953.

44] Between 28 and 31 August 1914 some 400 messages were intercepted and from 1 to 14 September, 1,300 interceptions helped to track the movements of the German armies.

Title : le lieutenant colonel George Housset, du pôle études et prospective du CDEC

Author (s) : le lieutenant colonel George Housset, du pôle études et prospective du CDEC

Release date 20/03/2020

FIND OUT MORE