Attention: Cyber!

military-Earth thinking notebook

le Lieutenant-colonel Stéphane DOSSÉ

Published on 16/06/2018

Sciences & technologies

At present, there are virtually no serious military operations without a cyber dimension. Yet warfare over telecommunications networks is frankly nothing new. Today's conflicts in cyberspace are merely the continuation of older conflicts dating from the late 19th and 20th centuries. For cyber warfare, it is also necessary to know the foundations of a past that allows for a correct understanding of the present.

The prehistory of current digital conflicts

Modern telecommunications were born with the electric telegraph, which, unlike the optical telegraph, makes it possible to free oneself from the constraints of the weather and the night. In just over a century and a half, from 1850 onwards, the cyber-electronic revolution transformed the battlefield. What some people perceive as new tactics, out of ignorance, are very often only updated versions of much older tactics, techniques or procedures, adapted to the technological novelty of the moment. Contemporary conflicts, since the Civil War, have thus shown that combat on networks is inseparable from any air-land or air-sea operation. The development of an objective and, above all, comprehensive analysis of the contribution of cyber-combat [1] to these new commitments often proves difficult, given the classification of documents and access to archives. Nevertheless, it is still possible to draw lessons from existing open sources.

The telegraph enters the art of warfare

The first military use (in the rear area) of the electric telegraph dates back to the American-Mexican War (1846-1848). It was used between different headquarters (Washington, Baltimore, Philadelphia, New York). The predominance of the United States, on the

military level, in the field of telecommunications, starts from this time.

Network combat led to a revolution in the art of warfare, of which the current cyber is only one evolution. The networking of the battle space began during the Crimean War (1853-1856), but there was little attack on telecommunications. Mobile electric telegraph stations were engaged by the French imperial forces (simultaneously with air telegraph stations) to link the expeditionary force to Paris. This made it possible to link the strategic level permanently or almost permanently to the tactical level.

The Civil War saw the emergence of the first network battles with the development of an operative command level and attacks against communications in depth. The electric telegraph is used from the strategic level (nationalization of private lines by President Lincoln for the war) to the tactical level (guiding artillery fire). As early as 1861, the telegraph arrived on the battlefield thanks to movable stations. Empirically appear the notions of deception on telecommunications, coding, intelligence, censorship, physical surveillance of vital networks, etc.. Coding was developed to protect communications, and the lines were monitored by patrols to counter Confederate attacks and various deteriorations carried out by Federal troops. Specialised units were even set up by the Confederate armies to destroy lines or carry out deception and eavesdropping operations - an innovation of this war - in the territory controlled by the Union. All in all, almost all current tactical network combat procedures have a proto-form in this conflict.

The Franco-Prussian War of 1870 marked a new stage in combat over telecommunications networks at the tactical level. The rigorous preparation of the Prussians and their German allies can be contrasted with French inventiveness. The latter undoubtedly avoids a total rout of the entire army. The actions to cut the cables and then to reuse them are systematized by the Germans at the operational level. Telegraphy was deployed on a large scale on both sides, including intelligence and deception actions (simulation, intrusion, intoxication) which were still limited to the tactical level. As they progressed, German reconnaissance cut the telegraph lines, which were rehabilitated by their telegraph services as soon as the stations reached the zone. The principle of neutralizing the most expensive enemy means of communication then appears more effective, for the later phases of the war, than their outright destruction [2]. The inadequacy of French military telegraphy (a company of telegraphers for the army) is offset by the courage, professionalism and patriotism of the civilians in the telegraph service. During the fall, some civilian operators served as contact observers and even infiltrated beyond enemy lines either to provide information or to re-establish communications with Paris, or to sabotage them. One example is Lemercier de Jauvelle's missions around Paris.

The first strategic-level battles, at sea and on land, for the control of telegraphy took place during the Spanish-American War of 1898 in the Philippine and Cuban theatres. The cutting of cables and the filtering of communications became an operating mode in its own right. The first recorded case of major destruction of cable for military purposes is believed to have occurred during the Battle of Manila Bay. On May[1], 1898, Commodore George Dewey engaged his fleet against the Spanish fleet, which he sank in a few hours. Realizing that the Spanish governor was using the only telegraph cable to communicate with his metropolis, he decided to cut this strategic means to isolate his opponent and promote the continuation of operations, after having proposed to the Spanish governor Primo de Rivera to consider it as neutral. The following cases occurred in the second theatre located in the region of Cuba. Between 11 May and 17 July, an operation - a veritable succession of attacks against telegraph infrastructures - was carried out by the

Americans. During this period, cables were also damaged between Haiti and Guantanamo. On 11 July, the last cable linking Santiago and Cienfuegos was also destroyed, finally isolating the Spanish forces.

British censorship of cables during the Boer War (1899-1902) also helped to show the world the strategic and tactical value of network warfare. This conflict and the Spanish-American War truly brought telecommunications into international conflicts on a level playing field. The role of the neutral powers was no longer negligible. It must be taken into account. A geopolitics of telecommunications thus emerges and revolutionizes both diplomacy and military strategy at the global level.

The appearance of new components of cyber-combatting

Professor Adolf Slaby, as early as 1897, predicted the use of jamming, whose first use in combat dates back to 1904 during the Russo-Japanese war, as does that of radio listening. On April 14, 1904, the Japanese battleships Kasuga and Nisshin bombed the Russian naval base of Port-Arthur, guided by smaller ships through a radio link. A Russian operator noticed this and decided to use his transmitter as a jammer. He thus neutralizes the Japanese action. During the naval battle of Tsushima, May 27 and 28, 1905, the Japanese use of listening to Russian radio communications, added to visual detection by a network of watch linked by radio, can identify the Russian fleet and thus participate directly in the decisive Japanese victory [3]. In less than seven years, electronic warfare has evolved from an academic possibility to effective operational use.

The two World Wars were an opportunity to improve all network warfare tactics based on older techniques (cable warfare, eavesdropping, censorship, deception, etc.).), and to develop techniques for locating (self or enemy): direction finding (World War I), then radar (World War II). For example, eavesdropping has a fundamental role in the victory of the Battle of the Marne [4] or in the halt of the great German offensive of June 9, 1918 [5] Tactical electronic warfare develops during trench warfare. At the end of the war, a French army had 10 to 18 listening posts. The security of communications naturally became a real issue from the First World War onwards, as the lessons of the wars of the previous two decades had not been fully learned. The Second World War confirmed the importance of electronic warfare. The deciphering of Enigma codes [6], the massive use of radars and H.F. direction finders contributed to a strategic victory in the Battle of the Atlantic. Tactical victories on land, sea and in the air are directly related to the control of the electromagnetic spectrum. The need to automate decryption operations and the development of the Manhattan Project lead to the development of the first computers that allow the calculation and storage of an ever-increasing amount of data. The world is slowly entering the digital age.

After the Second World War, the victors reorganized their services in the light of the Cold War and, for some, the wars of decolonization. The multiplication of conflicts and the development of telecommunications led to an explosion in the need for electromagnetic intelligence and international wiretapping. From time to time, military engagements require the regrouping of all combat capabilities on the networks, which in the 1960s took the name of electronic warfare. The digitisation of forces, which began timidly in the 1970s, became widespread in the 1990s and gradually made it necessary to adapt electronic warfare tactics to new techniques. At the same time, computer warfare

developed without these two fields being integrated, despite their striking similarities.

What can we infer from this?

Contemporary conflicts, from the American Civil War to the present day, have shown that combat on networks is inseparable from any air-land or air-sea operation. Moreover, telecommunications technology is clearly seen as a means and not an end in itself. The cyber phenomenon is no exception. Defeats and victories are primarily the consequences of decisions taken by leaders and cannot be attributed to technical means alone. However, failure to take full account of the use of the technology of one's time can quickly prove disastrous. Early wartime organizations that are deficient in this area are often one of the causes of defeat or, more broadly, reflect an intellectual and structural maladjustment to the war of the day. Nations or armies that have, at one time or another, been able to rapidly integrate telecommunications into their art of warfare have had a significant advantage, even if it is rarely decisive on its own over their enemies. The new telecommunications techniques when they appeared are systematically bypassed and fought against by the physical destruction of the supports (1st phase), then by intelligence [research] (2nd phase), and finally by a [search for] action on the enemy and protection of friendly networks (3rd phase). They very rarely lead to new military tactics.

The time has come for the digitisation of the operational area and the explosion of telecommunications and computer resources available to the population. The democratisation of telephony and information technology and the development of the civilian Internet will allow for increasing interaction between individuals. The current challenge is therefore not only to develop new tactics of war on the networks, but also to keep up with the evolution of information and communication technologies.and especially the democratization of the use of telecommunications, which has led to the democratization of the use of warfare in the last fifty years. The latest attacks from Stuxnet to Careto, the Snowden revelations and the Aramco affair show that this conflict remains very real. The current convergence of information technology and telecommunications is another step in a long process. The areas of combat on the networks (electronic warfare and cable warfare) were formerly separate for historical and personnel training reasons - cyber, on the one hand, and electronic, on the other. In the long run, it is clear that the convergence of wired and radio networks, combined with encryption, also implies a convergence of electronic warfare and cyber combat [7]. 7] Cyber-electronic support must therefore be fully integrated into the tactical and strategic thinking that sometimes evades it through ignorance...

1] Military confrontation in a cyberspace defined as the mesh of all the networks allowing the informational interconnection of living beings and machines.

[2] Steenackers F-F, "Telegraphs and posts during the war of 1870-1871"Carpenter Publisher, 1883, 620 pages.

[3] Price Alfred, "The history of US electronic warfare"The Association of Old Crows, 1984, Volume 1, Chap 1.

4] General Degoulange's articles on the website of the Army Electronic Warfare Association illustrate the subject well. ageat.asso.fr, consulted on 7 September 2013.

5] Lieutenant General Desfemmes, conference at the Special Military School of Coëtquidan "Reflections on electronic warfare",

published in the Revue de l'armée (No. 24 of December 62).

6] Message coding machines, used by the German forces.

7] Army looks to blend cyber, electronic warfare capabilities on battlefield, October 29, 2013, American Forces Press Service. FM 3-38 Cyber electromagnetic activities, www.fas.org/irp/doddir/army/fm3-38.pdf, 12 February 2014.

Stéphane DOSSÉ, Saint-cyrien, is an Army Signals Officer and a graduate of the École de guerre. Specialized in the field of information mastery, he draws on a wealth of operational experience. Also an engineer, he holds a Master's degree in network architecture from Télécom Paris Tech and a Master's degree in law in international security and defense from the University of Grenoble (UPMF). He has just published "Attention: cyber!"[1] with Aymeric Bonnemaison. He had previously published with Joffrey Guerry in DSI magazine (October 2011) "Combat dans le cyberespace: la bataille des câbles au XXIème siècle?" [2] with Aymeric Bonnemaison.

[1] Bonnemaison, Dossé, Attention: cyber! Vers le combat cyber-électronique, Economica, 2013. (see reading note page 65)

Title : le Lieutenant-colonel Stéphane DOSSÉ

Author (s) : le Lieutenant-colonel Stéphane DOSSÉ

Release date 01/06/2018