Attention: cyber !

cahier de la pensée mili-Terre

le Lieutenant-colonel Stéphane DOSSÉ

publié le 16/06/2018

Sciences & technologies

Actuellement, il n'existe pratiquement plus aucune opération militaire sérieuse sans dimension cyber. Pourtant, la guerre sur les réseaux de télécommunications n'est franchement pas une nouveauté. Les conflits actuels dans le cyberespace ne sont que la continuation de conflits plus anciens datant de la fin du XIX^{e} siècle et du XX^{e} siècle. Pour le combat cyber-électronique, il convient aussi de connaître les fondements d'un passé qui permet d'appréhender correctement le présent.

La préhistoire des conflits numériques actuels

Les télécommunications modernes naissent avec le télégraphe électrique, qui permet de s'affranchir de la contrainte de la météo et de la nuit, contrairement au télégraphe optique. En à peine plus d'un siècle et demi, à partir de 1850, la révolution cyber-électronique transforme le champ de bataille. Ce que certains perçoivent comme des tactiques inédites, par méconnaissance, ne sont bien souvent que les versions actualisées de tactiques, techniques ou procédures bien plus anciennes, adaptées à la nouveauté technologique du moment. Les conflits contemporains, depuis la guerre de Sécession, ont ainsi montré que le combat sur les réseaux est indissociable de toute opération aéroterrestre ou aéromaritime. L'élaboration d'une analyse objective et surtout complète de la contribution du combat cyber-électronique[1] à ces nouveaux engagements s'avère souvent difficile compte-tenu de la classification des documents et de l'accès aux archives. Il reste néanmoins possible de tirer des enseignements à partir des sources ouvertes existantes.

Le télégraphe entre dans l'art de la guerre

La première utilisation militaire (en zone arrière) du télégraphe électrique date de la guerre américano-mexicaine (1846-1848). Il est utilisé entre différents états-majors (Washington, Baltimore, Philadelphie, New York). La prédominance des États-Unis, sur le plan militaire, dans le domaine des télécommunications, commence dès cette époque.

Le combat sur le réseau a conduit à une révolution dans l'art de la guerre, le cyber actuel n'en constituant qu'une évolution. La mise en réseau de l'espace de bataille commence à l'époque de la guerre de Crimée (1853-1856), mais les télécommunications sont peu attaquées. Des stations mobiles de télégraphie électrique ont été engagées par les forces impériales françaises (simultanément à des stations de télégraphie aérienne) pour relier le corps expéditionnaire à Paris. Ceci permet de relier en permanence ou presque le niveau stratégique au niveau tactique.

La guerre de Sécession voit émerger les premiers combats sur les réseaux avec le développement d'un niveau de commandement opératif et d'attaques contre les communications dans la profondeur. Le télégraphe électrique est utilisé du niveau stratégique (nationalisation des lignes privées par le président Lincoln pour la guerre) au niveau tactique (guidage de tirs d'artillerie). Dès 1861, le télégraphe arrive sur le champ de bataille grâce à des stations déplaçables. De manière empirique apparaissent les notions de déception sur les télécommunications, de codage, de renseignement, de censure, de surveillance physique des réseaux vitaux, etc. Le codage est développé pour protéger les communications, et les lignes sont surveillées par des patrouilles pour contrer les attaques confédérées et les détériorations diverses effectuées par les troupes fédérales. Des unités spécialisées sont même mises sur pied par les armées confédérées pour détruire des lignes ou mener des opérations de déception et d'écoute – innovation de cette guerre – dans le territoire contrôlé par l'Union. En définitive, presque tous les procédés tactiques actuels de combat sur les réseaux ont une proto-forme dans ce conflit.

La guerre franco-prussienne de 1870 marque une nouvelle étape du combat sur les réseaux de télécommunications au niveau tactique. À la préparation rigoureuse des Prussiens et de leurs alliés Allemands, il est possible d'opposer l'inventivité française. Cette dernière évite sans doute une déroute totale de l'ensemble de l'armée. Les actions pour couper les câbles puis pour les réutiliser sont systématisées par les Allemands, au niveau opératif. La télégraphie est déployée à grande échelle dans les deux camps, y compris pour mener des actions de renseignement et de déception (simulation, intrusion, intoxication) qui se limitent encore au niveau tactique. Au fur et à mesure de leur progression, les reconnaissances allemandes coupent les lignes télégraphiques, qui sont réhabilitées par leurs services télégraphiques dès que les stations rejoignent la zone. Le principe de neutralisation des moyens de transmissions ennemis les plus coûteux apparaît alors plus efficace, pour les phases ultérieures de la guerre, que leur destruction pure et simple[2]. L'insuffisance de la télégraphie militaire française (une compagnie de télégraphistes pour l'armée) est palliée par le courage, le professionnalisme et le patriotisme des civils du service télégraphique. Durant l'automne, certains opérateurs civils servent d'observateur au contact et s'infiltrent même au-delà des lignes ennemies soit pour renseigner, soit pour rétablir les communications avec Paris, soit pour les saboter. Il faut citer en exemple les missions de Lemercier de Jauvelle autour de Paris.

Les premiers combats de niveau stratégique, maritimes et terrestres, pour le contrôle de la télégraphie ont lieu lors de la guerre hispano-américaine de 1898 sur les théâtres philippins et cubains. La coupure des câbles et le filtrage des communications deviennent des modes opératoires à part entière. Le premier cas répertorié de destruction majeure de câble dans un but militaire serait celui réalisé durant la bataille de la baie de Manille. Le 1er mai 1898, le Commodore George Dewey engage sa flotte contre la flotte espagnole qu'il coule en quelques heures. Comprenant que le gouverneur espagnol utilise l'unique câble télégraphique pour communiquer avec sa métropole, il décide de couper ce moyen stratégique pour isoler son adversaire et favoriser la suite des opérations, après avoir proposé au gouverneur espagnol Primo de Rivera de le considérer comme neutre. Les cas suivants surviennent sur le second théâtre situé dans la région de Cuba. Entre le 11 mai et le 17 juillet, une opération – véritable succession d'attaques contre les infrastructures télégraphiques – est conduite par les Américains. Durant cette période, des câbles sont également dégradés entre Haïti et Guantanamo. Le 11 juillet, le dernier câble reliant Santiago et Cienfuegos est lui aussi détruit, finissant d'isoler les forces espagnoles.

La censure britannique sur les câbles lors de la guerre des Boers (1899-1902) a aussi contribué à montrer au monde l'intérêt stratégique et tactique que constitue la guerre sur les réseaux. Ce conflit et la guerre hispano-américaine font véritablement entrer de plain-pied les télécommunications dans les conflits internationaux. Le rôle des puissances neutres n'est alors plus négligeable. Il doit alors être pris en compte. Une géopolitique des télécommunications apparaît ainsi et révolutionne au plan mondial tant la diplomatie que la stratégie militaire.

L'apparition de nouvelles composantes du combat cyber-électronique

Le professeur Adolf Slaby, dès 1897, prédit l'utilisation du brouillage, dont le premier usage au combat date de 1904 lors de la guerre russo-japonaise, tout comme celui des écoutes radio. Le 14 avril 1904, les cuirassés japonais Kasuga et Nisshin bombardent la base navale russe de Port-Arthur, guidés par de plus petits navires grâce à une liaison radio. Un opérateur russe s'en aperçoit et décide d'utiliser son émetteur comme brouilleur. Il neutralise ainsi l'action nippone. Lors de la bataille navale de Tsushima, les 27 et 28 mai 1905, l'exploitation japonaise des écoutes des radiocommunications russes, ajoutée à la détection visuelle par un réseau de guet relié par radio, permet de repérer la flotte russe et participe ainsi directement à la victoire décisive japonaise[3]. En moins de sept ans, la guerre électronique est passée d'une éventualité académique à un emploi opérationnel efficace.

Les deux guerres mondiales sont l'occasion d'améliorer toutes les tactiques de guerre sur les réseaux à partir de techniques plus anciennes (guerre des câbles, écoute, censure, déception, etc.), et de développer les techniques de localisation (de soi ou de l'ennemi): radiogoniométrie (Première Guerre mondiale), puis radar (Deuxième Guerre mondiale). Par exemple, les écoutes ont un rôle fondamental dans la victoire de la bataille de la Marne[4] ou dans l'arrêt de la grande offensive allemande du 9 juin 1918[5].La guerre électronique tactique se développe durant la guerre des tranchées. À la fin de la guerre, une armée

française dispose de 10 à 18 postes d'écoute. La sécurité des communications devient naturellement un véritable enjeu à partir de la Première Guerre mondiale, les enseignements des guerres des deux décennies précédentes n'ayant pas été pleinement tirés. La Seconde Guerre mondiale confirme l'importance prise par la guerre électronique. Le décryptage des codes Enigma[6], l'utilisation massive de radars et de radiogoniomètres H.F. contribue à obtenir une victoire stratégique lors de la bataille de l'Atlantique. Des victoires tactiques sur terre, sur mer et dans les airs sont liées directement à la maîtrise du spectre électromagnétique. Les besoins en automatisation des opérations de déchiffrement et le développement du projet Manhattan mènent au développement des premiers ordinateurs qui permettent le calcul et le stockage d'un nombre de plus en plus important de données. Le monde entre alors lentement dans l'ère du numérique.

Après la Seconde Guerre mondiale, les vainqueurs réorganisent leurs services dans l'optique de la guerre froide et, pour certains, dans celle des guerres de décolonisation. La multiplication des conflits et le développement des télécommunications impliquent une explosion des besoins en renseignement d'origine électromagnétique et en écoutes internationales. Ponctuellement, des engagements militaires nécessitent de regrouper l'ensemble des capacités de combat sur les réseaux, qui prend le nom de guerre électronique dans les années 1960. La numérisation des forces qui débute timidement dans les années 1970, se généralise dans les années 1990 et impose progressivement d'adapter les tactiques de guerre électronique aux techniques nouvelles. Simultanément, la lutte informatique se développe sans que ces deux domaines soient intégrés malgré des similitudes criantes.

Qu'en déduire?

Les conflits contemporains, depuis la guerre de Sécession jusqu'à aujourd'hui, ont montré que le combat sur les réseaux est indissociable de toute opération aéroterrestre ou aéromaritime. En outre, la technologie des télécommunications apparaît clairement comme un moyen et non une fin en soi. Le phénomène cyber n'y déroge pas. Les défaites et les victoires sont d'abord les conséquences de décisions prises par des chefs et ne peuvent être imputées aux seuls moyens techniques. Cependant, ne pas prendre en compte pleinement l'utilisation de la technologie de son époque peut s'avérer rapidement désastreux. Les organisations de début de guerre déficientes dans ce domaine sont souvent une des causes de défaite ou traduisent plus largement une inadaptation intellectuelle et structurelle à la guerre du moment. Les nations ou armées qui ont, à un moment donné, su intégrer rapidement les télécommunications dans leur art de la guerre ont eu un avantage significatif, même s'il est rarement décisif à lui seul sur leurs ennemis. Les nouvelles techniques de télécommunications à leur apparition sont systématiquement contournées et combattues par la destruction physique des supports (1ère phase), puis par une recherche de renseignement (2ème phase), et enfin par une recherche d'action sur l'ennemi et de protection des réseaux amis (3ème phase). Elles n'induisent que très rarement de nouvelles tactiques militaires.

L'heure est à la numérisation de l'espace des opérations et à l'explosion des moyens de

télécommunications et informatiques mis à disposition des populations. La démocratisation de la téléphonie, de l'informatique, et le développement de l'Internet civil permettront une interaction croissante entre les individus. L'enjeu actuel n'est donc pas uniquement de développer de nouvelles tactiques de guerre sur les réseaux, mais bien de suivre l'évolution des technologies de l'information et surtout la démocratisation de l'usage des télécommunications qui a induit la démocratisation de l'usage de la force guerrière dans les cinquante dernières années. Les dernières attaques de Stuxnet à Careto, en passant par les révélations Snowden et l'affaire Aramco, montrent que cette conflictualité reste bien réelle. L'actuelle convergence de l'informatique et des télécommunications constitue une nouvelle étape d'un long processus. Les domaines de combat sur les réseaux (guerre électronique et guerre des câbles) étaient anciennement séparés pour des raisons historiques et de formation du personnel – cyber, d'une part, et électronique, d'autre part. Dans le temps long, force est de constater que la convergence des réseaux filaires et radio, associés aux chiffrements, implique aussi une convergence de la guerre électronique et du combat cyber[7]. L'appui cyber-électronique doit donc être pleinement intégré dans les réflexions tactiques et stratégiques qui l'éludent parfois par méconnaissance...

[1] Affrontement militaire dans un cyberespace défini comme le maillage de l'ensemble des réseaux permettant l'interconnexion informationnelle des êtres vivants et des machines.

[2] Steenackers F-F, «Les télégraphes et les postes pendant la guerre de 1870-1871», Charpentier éditeur, 1883, 620 pages.

[3] Price Alfred, «The history of US electronic warfare», The association of Old Crows, 1984, Volume 1, chap 1.

[4] Les articles du Général Degoulange sur le site de l'association de la guerre électronique de l'armée de Terre illustrent bien le sujet. ageat.asso.fr, consulté le 7 septembre 2013.

[5] Général de corps d'armée Desfemmes, conférence à l'École spéciale militaire de Coëtquidan «Réflexions sur la guerre électronique», parue dans la Revue de l'armée (n° 24 de décembre 62).

[6] Machines de codage de messages, utilisées par les forces allemandes.

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

Stéphane DOSSÉ, Saint-cyrien, est officier des transmissions de l'armée de Terre et breveté de l'École de guerre. Spécialisé dans le domaine de la maîtrise de l'information, il s'appuie sur une riche expérience opérationnelle. Également ingénieur, titulaire d'un mastère spécialisé en architecture des réseaux de Télécom Paris Tech et d'un master de droit en sécurité internationale et défense de l'université de Grenoble (UPMF), il vient de publier «Attention: cyber!»[1] avec Aymeric Bonnemaison. Il avait auparavant publié avec Joffrey Guerry dans DSI magazine (octobre 2011) «Combat dans le cyberespace: la bataille des câbles au XXI^{ème} siècle?»

[1] Bonnemaison, Dossé, Attention: cyber! Vers le combat cyber-électronique, Économica, 2013. (voir note de lecture page 65)

Titre : le Lieutenant-colonel Stéphane DOSSÉ

Auteur(s) : le Lieutenant-colonel Stéphane DOSSÉ

Date de parution 01/06/2018