



Les origines historiques de la guerre électronique

2/2 - BRENNUS 4.0

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

publié le 19/03/2020

Sciences & technologies

« Va à Rome porter un message à César. Tu lui diras : « toute la Gaule est occupée ». Il te demandera : « toute ? ». Tu lui répondras : « toute ! », il comprendra ». Gosciny

C'est la crainte de « l'interception » qui est à l'origine du développement d'artifices destinés à camoufler les messages, que ce soit physiquement (on parle de stéganographie), soit par l'utilisation ou l'invention de codes et de chiffres, techniques utilisées pour déguiser le sens du message, afin que seul son destinataire désigné puisse le lire (on parle alors de cryptographie).

Hérodote[31] rapporte dans ses écrits la technique du tatouage du crâne des messagers tondus dont on laisse la chevelure repousser... procédé attribué au roi de Babylone Nabuchodonosor[32], surprenant et infaillible, mais long ! L'historien grec nous narre également l'histoire d'un ancien roi Spartiate réfugié auprès du roi des Perses, Xerxès. Mis au courant d'un projet d'invasion de la Grèce, il décide de prévenir Sparte en toute discrétion : « Il prit une tablette double, en gratta la cire, puis écrivit sur le bois même les projets de Xerxès ; ensuite il recouvrit de cire son message : ainsi le porteur d'une tablette vierge ne risquait pas d'ennuis ». En grattant la cire, comme en rasant la tête, le message en clair est transmis. Plus tard, on utilise les encres sympathiques (jus de citron, lait, certains produits chimiques ou même urine). Invisible à l'œil nu, une simple flamme, ou un bain dans un réactif chimique révèle le message. Une autre méthode consiste à dissimuler un message dans un texte. Il s'agit alors de piquer, de façon imperceptible, certaines lettres. Un autre procédé en usage chez les Chinois consiste à faire ingérer des boulettes de cire contenant des instructions aux messagers. Dans la « Guerre des Gaules », le grand César indique avoir fait usage de ce dernier procédé qui perdure au XXI^e siècle, comme tous ceux cités précédemment [33] et que l'on retrouve dans toutes les périodes troublées, du Moyen Âge à la Résistance, en passant par les guerres napoléoniennes.

Le premier des codes est naturel : le langage. Il a d'ailleurs depuis toujours représenté un

obstacle à la communication dans les armées faisant usage d'alliés, qu'elles soient romaines renforcées par les Germains, grecques complétées par des Gaulois ou napoléoniennes. C'est dans le but de résoudre ce problème général de compréhension qu'est né sur le champ de bataille « un langage de la musique » (tambours, cuivres), compréhensible par tous. Le plus étonnant est qu'au fil du temps et à la faveur du développement des technologies, l'homme a fait de cette faiblesse une force. Ainsi, pendant la Grande Guerre, les amérindiens de l'armée américaine (Choctaws et Cherokees) améliorent la sécurité des communications du front en communiquant par leur seule langue maternelle, incompréhensible des Allemands. Au cours du Second conflit mondial, les « code Talkers » sont des Comanches en France, des Meskwakis en Afrique du Nord et surtout des Navajos dans le Pacifique, dont la langue n'est alors pas écrite et dont la grammaire est des plus complexes[34]. Le « code » se montre impénétrable tout au long du conflit.

Qui est l'inventeur du premier code artificiel secret : les Indiens, les Chinois, les Égyptiens ? Les Grecs semblent en tout cas avoir été les premiers à se distinguer pour dissimuler leurs correspondances stratégiques. Dès le Ve siècle avant notre ère, les Spartiates inventent un algorithme dit de transposition, qui consiste à inverser l'ordre des lettres suivant un mécanisme. Ils emploient le scytate. Il s'agit d'un simple bâton autour duquel est enroulé, en spirale, un ruban de cuir ou de papyrus et sur lequel il suffit d'écrire dans le sens de la longueur. Une fois défait de son support, il est impossible de reconstituer l'ordre des lettres, sans posséder un bâton du même diamètre. Le message est porté comme une ceinture. Une des premières techniques de chiffrement employées par les hébreux, le Atbash, consiste en un algorithme de substitution de lettres. Il s'agit de remplacer une lettre de l'alphabet par une autre, suivant un ordre bien précis. Dans le cas présent : A devient Z, B devient Y etc. César utilise lui aussi un algorithme de substitution de lettres. Dans le cas du « chiffre de César », chacune des 26 lettres est remplacée par la lettre qui se situe trois positions plus loin de son rang dans l'alphabet. L'inconvénient de ce chiffrement par décalage est son peu de sûreté, puisqu'il n'y a que 25 possibilités de décalage. Le procédé est néanmoins utilisé par les officiers sudistes pendant la guerre de Sécession et par l'armée russe en 1915. Les dictionnaires chiffrés complètent les principaux systèmes de cryptographie militaires, on parle alors de chiffrement par substitution mono-alphabétique[36], qui consiste à remplacer une lettre par une autre, suivant une « table ».

Bientôt s'instaure un duel, depuis lors ininterrompu, qui oppose les inventeurs de chiffres et de clés aux cryptanalistes, briseurs de sceaux et de mystères. L'histoire nous enseigne que les seconds sont toujours victorieux. Certes, ils partent d'une feuille blanche, mais ils connaissent la langue de l'adversaire. Il n'y a que deux méthodes de déchiffrement : agir de manière empirique par essais et par erreurs, ou logiquement en tentant de comprendre l'algorithme de chiffrement, c'est-à-dire l'ordre logique des opérations de substitution ou de transposition qui composent le chiffrement. On traque alors ce qui peut s'apparenter à de la « similitude » et de la « régularité ». Les espaces et les fréquences entre les signes permettent de premiers soupçons. Après maints échecs, une lettre, un mot sont probablement découverts, puis vérifiés, en déduisent un second, puis un troisième. Lorsqu'éclate le Premier conflit mondial, il semble que le cerveau humain ait atteint une sorte de seuil dans les possibilités de chiffrement. On observe en effet que si plusieurs chiffres nouveaux apparaissent entre 1914 et 1918, ils relèvent tous de variantes ou de combinaisons des codes du XIXe siècle déjà déchiffrés. Ainsi, un nouveau code introduit par les Allemands en mars 1918 (le système ADFGVX), s'inspire d'un carré de l'historien grec Polybel[37], procédé qui remonte à l'Antiquité ! Le principe en est un chiffrement par substitution homophonique (pour éviter une analyse des fréquences, une lettre est remplacée par un symbole choisi au hasard parmi plusieurs). Le lieutenant Painvin[38], sorti major de l'Ecole Polytechnique en 1905, le décrypte in extremis en

quelques jours, alors que les Allemands sont à une centaine de kilomètres de Paris, ce qui permet au général Mangin[39] de mobiliser des troupes mises en réserve pour bloquer et repousser, au terme d'une bataille de cinq jours, la dernière offensive allemande.

La Seconde Guerre mondiale met un terme au cryptage/décryptage formulés manuellement. La matière grise ne suffit plus, on « mécanise l'abstraction » et on invente des machines qui pensent, pour vaincre des machines qui brouillent. Enigma[40] est une machine de chiffrement mécanique qui intègre une méthode de chiffrement par substitution polyalphabétique, c'est-à-dire une version améliorée du « chiffre de César ». Mais au lieu d'avoir une lettre systématiquement chiffrée par une autre, l'astuce dans la mécanique est d'introduire une clé qui permet de désigner la lettre à camoufler par plusieurs autres de façon aléatoire, ce qui complique le décryptage. Néanmoins, la machine a également ses faiblesses. Ainsi, la lettre A n'est jamais codée par un A et deux lettres différentes tapées à la suite ne donnent jamais, deux fois de suite, la même lettre chiffrée... cela élimine des combinaisons. Enigma est finalement vaincue par les Britanniques. Ces derniers procèdent par une logique fondée sur la connaissance du fonctionnement interne de la machine et l'exploitation des imprudences des chiffreurs allemands (envois de mots récurrents). Les Allemands disposent aussi du chiffrement Lorenz. Ce dernier est surtout utilisé par les hauts dirigeants allemands pour communiquer entre eux. Contrairement à Enigma, la machine de Lorenz peut coder chaque lettre de manière indépendante. « Les bombes électromécaniques », machines conçues pour décrypter les messages codés, ont finalement raison des deux moyens de chiffrement. À l'issue de la Seconde Guerre mondiale, Winston Churchill[41] écrit à l'attention du chiffre britannique : « jamais dans l'histoire, un si petit nombre d'hommes n'a tenu entre ses mains le destin d'un si grand nombre ».

Conclusion

La guerre électronique est, certes, une discipline récente apparue il y a un siècle. Mais lorsqu'on écrit en 2004 : « la guerre électronique, Maître des ondes, maître du monde... »[42], il ne s'agit que de la gradation d'un constat déjà formulé en 1992 par le général d'armée Marc Monchal, chef d'état-major de l'armée de Terre qui déclarait alors : « à l'avenir, le maître de l'électron l'emportera sur le maître du feu » ; propos qui s'apparentent, eux-mêmes à une déclaration de 1953 de l'ingénieur général Combaux qui prétendait déjà : « les télécommunications sont devenues le troisième élément fondamental de la guerre aussi important que le feu et le mouvement »[43]. Ainsi donc, si l'armée française est aujourd'hui confrontée à un nouveau défi de taille qui est celui de la guerre du cyberspace, la guerre de la communication a toujours arboré un visage protéiforme qui n'est pas fondamentalement différent des problématiques de l'heure.

En effet, on parle aisément aujourd'hui « d'un ennemi qui ne serait pas identifié », on semble regretter les guerres d'hier où « l'affrontement était physique » et on évoque « les nouvelles menaces, les cyber-attaques ». L'historicité nous rappelle précisément que dès l'Antiquité, l'ennemi n'était pas précisément identifié et que la guerre a toujours largement dépassé le périmètre de l'affrontement physique. Quant à la première cyber-attaque de l'Histoire, n'est-elle pas l'affaire de ces deux frères bordelais, fondateurs d'une société de placement, qui spéculent en bourse ? Grâce au soudoiment de quelques fonctionnaires, chargés de la communication entre Paris et Bordeaux, ils obtiennent, avant leurs concurrents, les informations venues de la bourse de Paris ce qui leur permet d'obtenir

de juteux bénéfiques. Nous ne sommes pas au XXe siècle et à l'heure d'Internet, mais en 1834 et le moyen de communication piraté est le télégraphe Chappe !

Ce dernier exemple ouvre un nouveau débat : l'histoire de demain est-elle déjà écrite ?

[31] Hérodote (485 av. J.-C./426 av. J.-C.), historien et géographe grec.

[32] Nabuchodonosor (600 av. J.-C./562 av. J.-C.).

[33] En 1980, il a été découvert une lettre de déporté écrite avec une encre de sympathie, décrivant les horreurs des camps.

[34] Le film « Windtalkers » (les messagers du vent), de John Woo, 2002, leur rend un vibrant hommage. Dans le film, Nicolas Cage a pour mission de protéger « le code », représenté par deux Indiens, et éviter qu'ils ne tombent aux mains de l'ennemi.

[35] Il est précisé que fort du retour d'expérience de la Première Guerre mondiale, Adolf Hitler diligente une trentaine d'anthropologues destinés à apprendre les langues amérindiennes, avant le Second conflit mondial. La tribu des Navajos est la seule à n'être pas étudiée et son langage est absolument incompréhensible pour les Européens, les Asiatiques et même les autres tribus. Ces particularités en font un « code secret » naturel sûr.

[36] C'est-à-dire le principe du « chiffre de César ».

[37] Polybe (200 av. J.-C./vers 118 av. J.-C.).

[38] Painvin Georges (1886-1980). Professeur à l'école des mines de Saint-Étienne, puis de Paris avant la guerre, géologue et paléontologue de formation, mais passionné par les « chiffres » il décrypte plus de 240 messages allemands pendant le conflit.

[39] Mangin Charles (1866-1925).

[40] On doit le brevet, qui date de 1919, à Hugo Koch (hollandais). L'allemand Arthur Scherbius crée la machine.

[41] Winston Churchill (1874-1965).

[42] Jean-Paul Siffre, général de l'armée de l'air, expert français de la guerre électronique. Son ouvrage paraît dans la collection « Renseignements et guerre secrète », Lavauzelle.

[43] Edmond Combaux, ingénieur général de 1ère classe, « électronique et guerre des ondes », Paris, 1953.

[44] Entre le 28 et le 31 août 1914 quelque 400 messages sont interceptés et du 1er au 14 septembre, 1300 interceptions contribuent à suivre les mouvements des armées allemandes.

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

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

Date de parution 20/03/2020

EN SAVOIR PLUS
