Au sein de la machine de guerre du Renseignement de l'armée britannique

Ce sont des soldats, mais la 77e Brigade monte des vidéos, enregistre des podcasts et rédige des messages viraux. Bienvenue à l'ère de la guerre de l'information

Par CARL MILLER,mercredi 14 novembre 2018
https://www.wired.co.uk/article/inside-the-77th-brigade-britains-information-warfare-military

Carl Miller est Directeur de Recherche au Centre pour l'Analyse des Médias Sociaux et auteur de "La Mort des Dieux : La Nouvelle Prise de Pouvoir Mondiale"

Future Publishing/Getty Images/WIRED

Une clôture de barbelés qui s'étire de part et d'autre. Un drapeau de l'Union qui flotte dans une rafale de vent, et des soldats qui rentrent et sortent de la guérite d'un garde au milieu de la route. Traversant la guérite, sous une rangée de projecteurs, je me suis dirigé vers une longue rangée de constructions basses de briques, ternes. On était à l'été 2017, et sur cette base militaire nichée au milieu des collines du Berkshire, je rendais visite à une section de l'armée britannique différente de toutes les autres. Il s'agit de la 77e brigade. Ce sont les troupes Britanniques qui mènent la guerre informatique de l'information.

"Si tout le monde pense de la même façon, alors cela veut dire qu'il y a quelqu'un qui ne pense pas ", voilà ce qu'on pouvait lire, en lettres d'un pied sur le tableau blanc d'un des principaux atriums de la base. D'un côté, il y avait une pièce remplie de grands blocs-notes électroniques et d'ordinateurs de bureau multi-écrans chargés de logiciels de montage numérique. Les hommes et les femmes de la 77e savaient installer des caméras, enregistrer du son, monter des vidéos. Ils venaient de tous les secteurs de l'armée et maîtrisaient la conception graphique, la publicité sur médias sociaux et l'analyse des données. Certains avaient suivi le cours de l'armée sur les opérations médiatiques de la Défense, et pratiquement la moitié d'entre eux étaient des réservistes issus de la société civile, employés à temps plein en marketing ou en recherche auprès des consommateurs.

D'un bureau à l'autre, j'ai trouvé des sections différentes de la brigade au travail. L'une des salles était consacrée à l'acquisition de la compréhension du public : la composition, la démographie et les habitudes des gens qu'ils voulaient atteindre. Une autre était plus analytique, se concentrant sur la création d'une " prise de conscience des attitudes et des sentiments " à partir d'un vaste ensemble de données sur les médias sociaux. Une autre encore était remplie d'agents produisant du contenu vidéo et audio. Ailleurs, des équipes de spécialistes du renseignement analysaient de près la façon dont les messages étaient reçus et discutaient des moyens pour les rendre plus percutants.

En expliquant leur travail, les soldats utilisaient des expressions que j'avais entendues des milliers de fois chez les spécialistes du marketing numérique : "influenceurs clés", "portée", "traction".Ce sont des mots qu'on entend

normalement dans les studios de publicité virale et les laboratoires de recherche numérique. Mais ici, les jeans Slim et les moustaches lissées avaient été remplacés par les chemises empesées et les camouflages légers de l'armée britannique. Leur environnement était tout aussi incongru - le quartier général de la 77e était un mélange de sols en linoléum, de longs couloirs et de portes coupe-feu. Plus Grange Hill que Menlo Park. A côté d'un studio de design numérique, les soldats faisaient une pause thé, un paquet de biscuits Digestives ouvert sur une boîte à munitions métallique verte. Sur une autre pancarte sur le mur on pouvait lire : " Changer les comportements est notre USP[argument de vente unique]". Mais au nom du ciel qu'est-ce qu'il se passait ici ?

"Si vous suivez à la trace les endroits où la main-d'œuvre britannique est déployée, vous pouvez avoir une bonne idée de l'endroit où on trouve ce genre d'activité " d'influence ", m'a dit plus tard un officier du renseignement(non affilié à la 77e), sous couvert d'anonymat. "Un document du ministère de la Défense va comporter des orientations générales et des thèmes à suivre." Il explique que maintenant, chaque campagne militaire a aussi - ou plutôt est - une campagne de marketing.

Depuis le déploiement des forces de l'OTAN dans les pays baltes en 2017, la propagande russe s'est également déployée, alléguant que les soldats de l'OTAN étaient des violeurs, des pillards, très peu différents d'une occupation hostile. L'un des objectifs de la guerre de l'information de l'OTAN était de contrer ce type de menace : réfuter sèchement les rumeurs préjudiciables et produire des vidéos des troupes de l'OTAN travaillant en bonne intelligence avec des hôtes baltes.

De telles campagnes d'information sont "blanches" : et sont ouvertement, avouons-le, la voix de l'armée Britannique. Mais, selon cet officier, pour des auditoires plus restreints, dans des situations de conflit, et si on jugeait que c'était proportionné et qu'il était nécessaire de le faire, les campagnes de messages pouvaient également devenir " grises " et " noires ". "Lutte contre la piraterie, les insurrections et le terrorisme ", a-t-il expliqué. Là-bas, il n'est pas nécessaire que le message ait l'air de venir de l'armée et même nécessairement qu'il dise la vérité.

Je n'ai rien vu qui prouve que la 77e soit engagée dans ce genre d'opérations, mais cette utilisation plus agressive du renseignement n'est pas nouvelle. Le GCHQ (Government Communication Headquarters = Centre de communication du Gouvernement), par exemple, dispose également d'une unité dédiée à la guerre de l'information. On l'appelle l' " Agence mixte de renseignement et de recherche sur les menaces" - ou JTRIG - un nom tout à fait obscur, comme c'est souvent le cas dans le monde du renseignement. Presque tout ce que nous savons à son sujet vient d'une série de diapositives divulguées en 2013 par Edward Snowden, le lanceur d'alerte de la NSA. Ces documents nous donnent un aperçu de ce que peuvent être de telles campagnes secrètes d'information.

Selon les diapositives, la JTRIG avait pour mission de discréditer les entreprises, en transmettant "des informations confidentielles à la presse par le biais de blogs, etc." et en publiant des informations négatives sur des forums Internet. Ils pouvaient changer les photos de quelqu'un sur les médias sociaux (comme le précisait une diapositive : "de quoi amener la 'paranoïa' à un niveau inédit ".) Ils pouvaient utiliser des techniques de type duperie - c'est-à-dire : placer des informations " secrètes " sur un ordinateur compromis. Ils leur était possible de bombarder de SMS ou d'appels le téléphone de quelqu'un.

JTRIG disposait également d'un arsenal de 200 armes d'information, allant d' armes en cours de développement aux armes pleinement opérationnelles. Un outil appelé " Blaireau " permettait l'envoi massif de courriels. Un autre, appelé "Burlesque", parodiait des messages SMS. "Clean Sweep" imitait des posts Facebook pour des individus ou des pays entiers. "Gateway" permettait "d'augmenter artificiellement le trafic vers un site web". "Underpass" était un moyen de changer les résultats des sondages en ligne.

Ils avaient des objectifs opérationnels dans le monde entier : Iran, Afrique, Corée du Nord, Russie et Royaume-Uni. Parfois, les opérations se concentraient sur des individus et des groupes spécifiques, parfois sur des régimes plus vastes ou même sur des populations en général. L'Opération Quito a été une campagne menée peu après 2009 pour empêcher la reprise des îles Falkland par l'Argentine. Selon une diapositive " espérons que cela débouche à long terme sur une opération novatrice de grande échelle". A partir de mars 2011, une autre opération avait pour objectif le renversement du régime du Zimbabwe en discréditant le parti Zanu PF.

Une balade au sein du quartier général de la 77e, laissait voir l'étalage de l'étrange nouvelle réalité de la guerre . Nous avons tous beaucoup entendu parler de la "guerre cybernétique", c'est-à-dire de la façon dont les États pourraient s'attaquer à leurs ennemis au moyen de réseaux informatiques, en endommageant leur infrastructure ou en volant leurs secrets. Mais ce n'était pas ce qui se passait ici. Ici, au sein de la 77e Brigade, il s'agissait d'une guerre de story-boards et de récits, de vidéos et de médias sociaux. Ce n'est plus seulement sur le champ de bataille que se font les affrontements, c'est aussi dans les médias et en ligne. Une victoire se gagne autant par les yeux du public que par des armées adverses sur le champ de bataille. La guerre à l'ère de l'information est une guerre contre l'information elle-même.

Propagande publiée sur Facebook par des agences de relations publiques russes pour tenter d'influencer l'élection présidentielle américaine de 2016 Credit Facebook

Il y a plus d'une décennie, et bien loin de la 77e Brigade, il y avait des gens qui savaient déjà que l'Internet était un nouvel outil d'influence puissant. Ce qu'ils faisaient ne s'appelait pas "guerre de l'information", opérations médiatiques, activités d'influence, action en ligne ou tout autre langage militaire qu'il était appelé à devenir. Les membres de ces sous-cultures en ligne en ébullition qui s'agglutinaient autour des forums de piratage, dans les CRI (Centre de Recherche Internationaux) et forums à images comme 4chan, aurait pu appeler cela "piratage de l'attention". Ou tout simplement lulz (Version moins sympathique de LOL = Laugh out loud = rires. Lulz est plus dédaigneux, sarcastique NDT).

En 2008, Oprah Winfrey a averti ses millions de téléspectateurs qu'un réseau pédophile connu "a plus de 9 000 pénis et que tous sont des violeurs d'enfants". Or ça, c'était une blague de 4chan (forum anglophone anonyme NDT) sur le thème de Dragon Ball posté sur le forum de l'émission. Un an plus tard, le magazine Time a effectué un sondage en ligne pour que ses lecteurs choisissent les 100 personnes les plus influentes du monde, et 4chan a utilisé des scripts pour truquer le vote afin que son fondateur - Christopher Poole, alors âgé de 21 ans, communément appelé "moot " - arrive en premier. Ils ont construit des robots et des "sockpuppets" - faux comptes de médias sociaux pour rendre les sujets tendances et les faire paraître plus populaires qu'ils ne l'étaient - ils se sont regroupés pour submerger leurs cibles. Ils ont commencé par se servir des ordinateurs pour changer ce que les gens voyaient, et peut-être même ce qu'ils pensaient. Ils ont célébré chacune de leurs victoires avec un déluge de memes.

D'autres ont rapidement attaqués les lulz pour l'argent. Tout au long des années 2000, les petites sociétés de relations publiques, les cabinets de conseil en communication politique et les marchés darknet ont commencé à vendre les tactiques et les techniques mises au point sur 4chan. "Des marchands calés en médias numériques militarisent leur connaissance des services de manipulation des médias sociaux ", me dit sous couvert d'anonymat un chercheur en cybersécurité qui suit ce type d'activité commerciale illicite .

"C'est comme un travail à la chaîne, poursuit-il. "Ils préparent la campagne, pénètrent le public cible, maintiennent l'opération, puis se désengagent stratégiquement. Cela ne fera que s'amplifier."

Nombre de sites Web ont commencé à vendre de faux comptes, décrits, catégorisés et évalués presque comme du vin : de la piquette bon marché jusqu'aux millésimes réputés. L'"ÉNORME MEGA BOT PACK", disponible pour seulement 3 $ sur le darknet, vous permettait de construire votre propre armée de bots sur des centaines de plate formes de médias sociaux. Il y avait des services pour manipuler les résultats des moteurs de recherche. Vous pouviez acheter des articles Wikipédia. Vous pouviez louer de fausses adresses IP pour faire croire que vos comptes provenaient du monde entier. Et au sommet du marché se trouvaient les "fermes de légendes", des entreprises qui exploitent des dizaines de milliers d'identités uniques, chacune avec des comptes multiples sur les médias sociaux, une adresse IP unique, sa propre adresse Internet, et même sa propre personnalité, ses intérêts et son style d'écriture. Le Lulz s'était métamorphosé en un modèle de business.

Au sein de la base de la 77ème, tout était en mouvement. Les planchers étaient posés, les unités de travail installées ; les bureaux - vides de biens personnels - formaient des lignes nettes dans les bureaux encore recouverts de plastique, de ruban adhésif et de sciure de bois. L'unité a été formée à la hâte en 2015 à partir de diverses parties plus anciennes de l'armée britannique - Groupe des Opérations Médias, Groupe de Soutien à la Stabilisation Militaire, Groupe des Opérations Psychologiques. Depuis, elle n'a cessé de croître rapidement.

En 2014, un an avant la création de la 77e, une note de service intitulée "La guerre à l'ère de l'information" a circulé au sein de l'armée britannique . "Nous sommes maintenant aux contreforts de l'ère de l'information", annonçait le mémo. Il faisait valoir que l'armée britannique avait besoin de mener un nouveau type de guerre, une guerre dont " l'information serait le point central ". Comme le précisait le mémo, l'Armée devait être présente sur les médias sociaux, sur Internet et dans la presse " afin d'être la première à dire la vérité, de contrer les récits des autres et, au besoin, de manipuler l'opinion de milliers de personnes simultanément pour appuyer des opérations de combat, dans la réciprocité et en temps réel."

Puis cette affaire de Lulz 'est devenue une question de géopolitique. Partout dans le monde, les militaires en sont venus exactement à la même conclusion que les Britanniques, et souvent plus rapidement. La première ligne de la Doctrine interarmées alliée pour les opérations d'information de l'OTAN, publiée en 2009 précise : "Il y a vis à vis de l'information une réelle appétence, mais aussi une dépendance accrue". Et elle est arrivée à la même conclusion que le mémo militaire Britannique : il fallait une "attention accrue quand aux opérations d'information" en temps de guerre. Pour le dire plus simplement, il fallait utiliser les opérations d'information pour cibler la volonté de l'ennemi. "Par exemple, en remettant en question la légitimité du leadership et de la cause, les activités du renseignement peuvent miner leur socle de pouvoir moral, séparant les dirigeants de leurs partisans, politiques, militaires et publics, affaiblissant ainsi leur volonté de poursuivre et affectant leurs actions ", explique le document.

La Russie, elle aussi, était de la partie. Le Printemps Arabe, les révolutions dans plusieurs États post-soviétiques, l'élargissement de l'OTAN - chacun d'entre eux s'était effondré face à l'émiettement de la puissance russe. La Russie disposait d'une grande armée conventionnelle, mais cela n'avait plus la même importance que dans le passé. Le chef de l'état-major général russe, Valery Gerasimov, a commencé à réviser ce qui relevait du militaire. La guerre, a-t-il dit dans un article de Voyenno-Promyshlennyyy Kurier (The Military Industry Journal), est désormais "hybride" - brouillant les frontières entre guerre et paix, le civil et le militaire, l'étatique et le non étatique. Et il existait un autre flou : entre la force et les idées. La " lutte morale, psychologique, cognitive et informationnelle ", comme l'a dit Gerasimov, est maintenant fondamentale lors de conflits.

Nous savons maintenant à quoi ressemble la guerre de l'information russe. Moscou a construit un appareil qui va des médias grand public aux coulisses de la blogosphère, du Président de la Fédération de Russie à l'humble robot. Tout comme les premiers pirates de l'attention, leurs techniques sont un mélange du très visible et du très secret - mais à une échelle bien plus vaste.

Cependant, le regard occidental s'est révélé moins attentif quand d'autres théâtres de guerre de l'information non anglophones ont éclaté. Gerasimov avait raison : chaque cas était un cas de frontières floues. C'était une guerre de l'information, mais pas toujours menée uniquement par des militaires. Elle était menée par l'État, mais comprenait aussi parfois de nombreux acteurs non étatiques. Il s'agissait avant tout d'actes interne au pays, commis par des autocrates, visant leur propre population.

Un article de Harvard publié en 2017 estimait que le gouvernement Chinois emploie deux millions de personnes pour écrire, chaque année, 448 millions de messages sur les médias sociaux. Leur but premier est d'écarter les sujets politiques sensibles des débats en ligne. Marc Owen Jones, chercheur à l'Institut d'Études Arabes et Islamiques de l'Université d'Exeter, a mis au jour des milliers de faux comptes Twitter en Arabie Saoudite, "tout à la gloire du gouvernement saoudien ou de sa politique étrangère". Au Bahreïn, on a vu que des opérations de type spam avaient été menées, visant à empêcher les dissidents de se retrouver ou de débattre en ligne de sujets politiquement dangereux. Au Mexique, environ 75 000 comptes automatisés sont connus localement sous le nom de Peñabots, du nom du président Enrique Peña Nieto, inondant les hashtags de protestation d'informations non pertinentes et ennuyeuses afin d'enterrer toute information utile.

Voilà des milliers d'années que la désinformation et la tromperie font partie de la guerre, mais partout dans le monde, il y avait quelque chose de nouveau. Pendant longtemps, l'information a été utilisée comme appui des opérations de combat, aujourd'hui, on considère que c'est par son intermédiaire que les combats se déroulent principalement, parfois même exclusivement. Les armées se sont rendu compte que d'outil de guerre, l'information est devenue guerre elle même, le combat se faisant au delà et par l'information. Et ce n'était pas confiné à la Russie, à la Chine ou à qui que ce soit d'autre. Une lutte mondiale de l'information a éclaté. Des dizaines de pays en font partie. Et il ne s'agit là que de ce dont nous avons connaissance.

Les soldats de la 77e Brigade portent à leur épaulette un petit insigne rond, de couleur azur, encerclant une créature d'or rugissante, ressemblant à un lion. Appelée Chinthe, c'est un animal mythique d'origine birmane arborée en premier par les Chindits, force de guérilla britannique et indienne créée pendant la Seconde Guerre mondiale pour protéger la Birmanie contre l'avancée de l'armée Nippone. Une armée d'irréguliers, les Chindits s'infiltraient loin à l'intérieur des lignes ennemies lors de sorties imprévisibles, détruisant les dépôts de ravitaillement et coupant les liaisons de transport, visant à semer la confusion autant que la destruction.

Ce n'est pas un hasard si les gars de la 77e arborent le Chinthe sur l'épaule. Comme les Chindits, ils constituent un nouveau type de force. Un modèle peu orthodoxe, mais aux yeux de l'armée britannique une innovation nécessaire; qui reflète simplement le monde dans lequel nous vivons tous aujourd'hui et le nouveau type de guerre qui s'y déroule.

Cette nouvelle forme de guerre pose un problème que ni la 77e Brigade, ni l'armée, ni aucun État démocratique n'ont encore résolu. Il est facile de trouver comment tromper les publics étrangers, mais beaucoup, beaucoup plus difficile de savoir comment protéger les nôtres. Qu'il s'agisse de la participation de la Russie aux élections américaines, au Brexit, de l'empoisonnement au novichok ou des dizaines d'autres exemples que nous connaissons, les cas se multiplient. Dans la guerre de l'information, c'est par sa conception même que l'offensive l'emporte presque systématiquement sur la défense. Il est bien plus facile de fabriquer des mensonges que de convaincre tout le monde que ce sont des mensonges. La désinformation n'est pas onéreuse; la discréditer est ruineuse et complexe.

Plus grave encore, ce type de guerre profite davantage aux États autoritaires qu'aux États démocratiques libéraux. Pour les États et les militaires, manipuler Internet est d'un coût dérisoire et c'est facile à faire. Le facteur qui pourrait le limiter n'est pas technique, mais légal. Et quels que soient les dérapages des services de renseignement occidentaux, ils continuent d'opérer dans des environnements juridiques qui tendent à limiter plus encore où et dans quelle mesure la guerre de l'information peut être déployée. La Chine et la Russie n'ont pas de tels obstacles juridiques.

Nous doter tous des compétences nécessaires pour nous protéger de la guerre de l'information est peut-être la seule véritable solution au problème. Mais cela prend du temps. Et ce qui serait enseigné ne pourrait pas suivre le rythme de ce qu'il est possible de faire. Dans l'état actuel des choses, les possibilités technologiques, dépassent de loin la compréhension du public.

On construisait souvent le Chinthe à l'entrée des pagodes, des temples et autres sites sacrés pour les protéger des menaces et des dangers de l'extérieur qui les guettaient. Aujourd'hui, ce site sacré, c' est l'Internet lui-même. Du lulz au spam, en passant par la guerre de l'information, le poids de ce qui la menace est beaucoup mieux financé et plus puissant. L'ère de la guerre de l'information ne fait que commencer.