19 novembre 2014
LE HUFFINGTON POST
EN ASSOCIATION AVEC LE GROUPE Le Monde

Sonia Eyaan Devenez fan
Journaliste et consultante en Stratégie Digitale

Cyber-jihadisme: la guerre électronique contre Daech est-elle perdue d'avance?

Publication: 19/11/2014 07h42 CET Mis à jour: il y a 2 heures

Twitter, LiveLeak, Snaptchat ou Facebook, de nombreux réseaux sociaux et blogs sont utilisés par les organisations salafiste-jihadistes pour déployer "leurs campagnes de relations publiques". Alors que la riposte des Alliés sur ces nouveaux champs de bataille est en marche, revenons sur les principaux enseignements à tirer du cyber-jihadisme.

Autant le dire tout de suite, pour Bradley Manning, ce troisième volet de la guerre en Irak destiné à détruire l'organisation État islamique (EI) par le recours aux frappes aériennes est voué à l'échec. Dans un article du Guardian publié en septembre dernier, le soldat américain réputé pour avoir divulgué à Wikileaks plus de 700 000 documents confidentiels de l'armée américaine explique que cette offensive ne fera qu'alimenter "le cycle d'indignation, de recrutement, d'organisation et de combats qui existe depuis des décennies".

Les réseaux sociaux au cœur de la guerre contre Daech

Parmi les solutions que préconise Bradley Manning - devenu Chelsea Manning - figure la lutte contre l'embrigadement, le recrutement et la formation de jeunes sur les réseaux sociaux. Manifestement, le soldat de 26 ans peut se réjouir. En France, l'article 9 de la loi antiterroriste adoptée par l'Assemblée Nationale le 30 octobre 2014 contient un dispositif bloquant l'accès aux sites faisant l'apologie du terrorisme. Outre l'alliance militaire, les États-Unis ont par ailleurs annoncé lundi 27 octobre la création d'une cyber-coalition réunissant des pays occidentaux et des pays musulmans. Même les hackers d'Anonymous participent au combat contre l'EI en lançant courant septembre l'"Operation Ice ISIS". Cette initiative vise à protéger les individus potentiellement menacés par les djihadistes sur le Net et dans le monde réel. L'autre but de l'opération est de faire barrage à l'expansion de l'idéologie des terroristes islamistes sur les réseaux sociaux.

Mais attention, il ne s'agit pas de crier victoire trop tôt. En août 2013, Khalil Shreateh un expert palestinien en sécurité, a publié un message sur le mur de Mark Zuckerberg pour démontrer qu'il existait une faille de sécurité permettant à n'importe qui de diffuser des

messages sur le mur d'une autre personne sans y avoir été autorisé. Il est aisé d'imaginer combien l'usage de ce type de faille par des groupuscules terroristes pourrait s'avérer dangereuse. D'autant plus qu'en dehors des aspects techniques,d'après le Financial Times, les djihadistes du groupe État islamique (EI) se sont récemment imposés des règles de "bonne conduite" sur les réseaux sociaux afin de ne pas se faire géolocaliser via des tweets ou des post Facebook. Les chefs de l'EI ont également demandé aux combattants de ne pas publier des tweets contenant des lieux ou des noms de personnes suivant le Daily Mail. A l'inverse, du côté des Alliés, la "coalition de l'information" semble pour l'instant patiner. C'est ce que semble dire à mots couverts Robert Hannigan dans une chronique du Financial Time du 3 novembre. Le nouveau patron du GCHQ, le service de renseignement électronique du gouvernement britannique accuse les entreprises américaines de l'Internet "d'être devenues des centres de contrôle et de commandement privilégiés pour les terroristes et les criminels".

Le Califat numérique: une toile d'araignée aux multiples ramifications

Et pourtant il est urgent que les géants de la Silicon Valley coopèrent davantage dans la lutte contre l'EI. Car en plus des réseaux sociaux, les djihadistes investissent dans des outils de chiffrement sophistiqués et utilisent des techniques de stéganographie ingénieuses, parfois même scabreuses, pour protéger leurs communications. En mai 2011, Masqood Lodin, un membre présumé d'Al-Qaïda est arrêté à Berlin avec en sa possession une carte mémoire et une clé USB contenant à première vue une vidéo à caractère pornographique intitulée "KickAss", et un fichier nommé "Sexy Tanja". Un an plus tard, CNN révèle que les supports de stockage de l'Autrichien dissimulaient plus de 100 documents d'Al-Qaïda présentant des plans, des manuels d'entraînement et des opérations en préparation ou déjà réalisées.

Ne nous méprenons donc pas: la cyberguerre menée par les organisations salafiste-jihadistes s'étend bien au-delà des réseaux sociaux. Selon un article de Fox News publié en septembre dernier, Junaid Hussain alias Abu Hussain Al Britani, un hacker britannique réputé pour avoir piraté le compte Gmail de l'ancien Premier ministre britannique Tony Blair, a rejoint l'EI et s'est lancé dans une campagne de recrutement destinée à convaincre des musulmans radicaux passionnés d'informatique à s'enrôler en Syrie. Toujours selon le même article, de nombreux experts en sécurité soutiennent que l'organisation État islamique se prépare à frapper les infrastructures des pays occidentaux. Imaginons le climat d'inquiétude voire de panique dans lequel serait plongée la France si des réseaux électriques, des hôpitaux et des banques étaient simultanément mis hors services, et la désorganisation qui en résulterait. Imaginer un tel scénario peut donner l'impression de sombrer dans le catastrophisme parce que nos infrastructures économiques nous semblent, pour détourner un concept économique bien connu, "too big to fall". Mais s'il survenait, un remake 2.0 de l'attentat du 11 septembre 2001, les conséquences socioéconomiques et psychologiques seraient désastreuses à l'échelle planétaire. À noter que la cyberattaque subie en 2007 par l'Estonie montre que ce scénario n'est pas qu'une simple vue de l'esprit.

La vraie question est donc de savoir si les USA et l'Europe sont parés pour déjouer des attaques cybercriminelles d'envergure? Pas si sûr à en croire Richard Clarke. Le célèbre conseiller antiterrorisme de la Maison Blanche qui a démissionné en 2003 pour protester contre la guerre en Irak explique lors du World in 2013 Festival qu'il est bien plus simple pour les Etats-Unis de lancer une cyberattaque que de mettre en place une stratégie de cyberdéfense. Olivier Velin, expert en sécurité des systèmes d'information souligne par ailleurs que "pour un groupuscule bien formé, les nombreuses failles existantes sur l'Internet sont autant de portes ouvertes et d'incitations à agir contre les intérêts d'autrui de la façon la moins coûteuse". En effet, ajoute-t-il, "dans la très grande majorité des organismes et entreprises des secteurs public et privé, le respect des procédures de sécurité est perçu par les utilisateurs comme une contrainte inutile qui complique le travail et ne procure aucun avantage évident." Et dans les faits, "la sécurité est l'un des premiers budgets sacrifiés lors des coupes budgétaires. Or, la mise à niveau des dispositifs de sécurité doit suivre l'évolution des technologies et des versions de logiciels".

En dehors même des procédures de sécurité, il est bon de souligner que le Darknet occupe une place non négligeable dans cette cyberguerre. Il faut savoir en effet que les moteurs de recherches dont Google, Amazon, Yahoo ou Qwant ne contiennent qu'une infime partie des informations de l'Internet. En réalité près de 96% des données du World Wild Web circulent sous la protection de l'anonymat offert par des réseauxcomme Tor, FreeNet ou I2P. Cette agora virtuelle développée à l'origine par l'US Navy pour sécuriser les communications militaires est aujourd'hui utilisée par des journalistes, des hackers ou des dissidents politiques souhaitant contourner la surveillance ou la censure de régimes totalitaires. Le nœud du problème est que le Darknet permet également aux pédophiles, aux acheteurs d'armes, aux narcotrafiquants et autres terroristes de passer plus facilement entre les mailles du filet. Les choses pourraient changer à en croire les révélations de journalistes des chaînes de télévision publiques allemandes, selon qui la NSA aurait utilisé le logiciel anti-cybercriminalité XKeyScore pour surveiller et collecter des données d'utilisateurs de Tor en Allemagne Pour Olivier Velin, "mettre en œuvre des dispositifs destinés à espionner chaque citoyen comme s'il était un terroriste en puissance est difficile à accepter pour la plus grande majorité des populations concernées."

L'Occident a-t-il renoncé à son leadership idéologique?

Mais que voulez-vous nous sommes en guerre. À ce stade, seul l'avenir nous dira si la contre-offensive des alliés rencontre un franc succès. Car aujourd'hui encore ce sont près de 1000 combattants étrangers, dont des français en 5ème position, qui continuent d'affluer en Syrie d'après Le Parisien. Mais pour l'heure, une dernière question mérite d'être posée. Pour quelles raisons l'appel au combat des moudjahidines - morbide parodie de l'appel pacifique du muezzin à la prière - rencontre un écho non négligeable dans les pays occidentaux? Certains diront que ces organisations s'adressent à des jeunes en situation difficile faisant une mauvaise lecture du Coran. Dans une interview accordée

à la BBC, un ancien djihadiste Danois soutien que George W. Bush "a poussé des milliers" de personnes dans le terrorisme en disant: "Vous êtes avec nous, ou contre nous". Difficile de ne pas faire allusion au discours de Georges W Bush sur l'importance de la démocratie au Moyen-Orient et de la guerre au terrorisme prononcé en février 2004 devant le Congrès Américain. Difficile également de nier avec le recul que la révélation de la non-existence d'arme biologique et chimique de destruction massive en Irak a joué un rôle dans l'essor du cyber jihadisme. Pour mieux comprendre il faut revenir en 2006, année de l'arrivée sur la toile de Wikileaks. L'objectif de la plateforme créée par Julien Assange étant de divulguer des documents confidentiels - notamment sur les guerres d'Irak et d'Afghanistan - afin de palier à l'asymétrie d'information qui existe entre les pouvoirs publics et les citoyens. Rapidement la presse mondiale s'empare du phénomène WiKileaks et les bavures de l'armée américaine en Irak se partagent sur les réseaux sociaux. Pour l'anecdote, le fait que le vice-président Biden ait traité Julian Assange de "terroriste hi-tech" en 2010, et que la même année le fondateur de Wikileaks soit élu personnalité de l'année par les internautes du Time illustre le climat de défiance qui pèse sur les politiques depuis le mensonge d'État du président Bush. Et bien que les données brutes de WikiLeaks sont incompréhensibles pour une grande partie des citoyens, reste que Julien Assange a contribué à l'essor des whistleblowers sur l'Internet et les réseaux sociaux.

Pour en revenir au cyber-jihadisme, tel le miroir inversé de la rhétorique bushienne, c'est précisément leur vision de "l'axe du bien en lutte contre l'axe du mal" que les moudjahidines tentent d'imposer à coup de tweets. Si cette comparaison est un brin douteuse, elle suggère néanmoins que depuis quelque temps les grandes métavaleurs occidentales de paix, de tolérance et de liberté ont pris des couleurs pâles et froides. Et à regarder de plus près c'est notre idéologie du bien-être consumériste qui s'enlise dans cette guerre de l'information et de la désinformation. Mais on a beau tendre l'oreille, nulle alternative au fameux "vous êtes avec nous ou contre nous » ne semble venir de chez l'Oncle Sam ni de ses cousins européens. Et pourtant, la France des Lumières et du Général de Gaulle gagnerait à se démarquer de la position dominante jugée parfois jusqu'au-boutiste. Loin est le temps semble-t-il où la posture occidentale consistant à proclamer quelques grands principes humanistes sans s'embarrasser de leur mise en œuvre suffisait.

Suivre Sonia Eyaan sur Twitter: www.twitter.com/Eyaansonia

PLUS:

DaechCyber JihadismeInternational WikileaksIdéologieTerrorismeRéseaux Sociaux