Comment Google et la Silicon Valley contribuent au maintien de l'empire américain

Quand les médias ont braqué leurs projecteurs sur les mouvements critiques de la Silicon Valley, c'était pour pointer la hausse des loyers à San Francisco ou son aide apportée à la NSA. Cependant, ces maigres pointes émergées n'entachent pas la réputation de bienveillance et de progressisme de la Silicon Valley : elle n'est toujours pas considérée comme aussi néfaste que *Wall Street* ou les grands groupes pétroliers. Pourtant la « Surveillance Valley » est totalement liée à l'armée américaine, aux services de renseignements et aux fournisseurs de la Défense. Militarisme technologique, drones, espionnage, robots et opérations contre-insurrectionnelles, nous ne publions pas cette traduction d'un article américain pour dénoncer les seuls agissements de l'Oncle Sam, mais ceux de l'industrie technologique en général, qu'elle soit française, chinoise, russe ou iranienne.

Un aspect de la Silicon Valley qui ternirait sa réputation n'a pas été assez examiné : son implication dans le militarisme américain. Les liens entre la Silicon Valley et la Sécurité Nationale s'étendent au-delà du programme PRISM de la NSA. *Via* de nombreux partenariats et contrats avec les organismes militaires, les services de renseignement et de police, la Silicon Valley fait partie du complexe militaro-industriel américain. Google vend ses technologies à l'armée US, au FBI, la CIA, la NSA, la DEA [agence anti-drogue], la NGA [agence géospatiale] ainsi qu'à d'autres agences de renseignement et de police. Ses directeurs ont par le passé travaillé dans l'armée et le renseignement. Google s'associe avec des fournisseurs de la Défense comme Lockheed Martin et Northrop Grumman. Amazon a conçu une plate-forme de *cloud*[1] qu'utiliseront la CIA et toutes les autres agences de renseignement. La compagnie Palantir financée par la CIA vend son programme d'exploration et d'analyse de données à l'armée US, à la CIA, aux polices de New-York et de Los Angeles et à d'autres agences de sécurité. Ces technologies comprennent des applications destinées aux zones de combat et à l'espionnage.

D'abord, un peu d'histoire pour expliquer les relations entre l'armée et la Silicon Valley depuis la conception de ce centre technologique. Les origines de la Silicon Valley remontent à la deuxième guerre mondiale, d'après la présentation qui en est faite par le chercheur et entrepreneur Steve Blank.[2] Pendant la guerre, le gouvernement US a financé un labo secret à Harvard pour chercher un moyen de brouiller le système électronique de défense aérienne guidé par radar des Allemands. La solution : larguer du papier aluminium devant les radars allemands pour les bloquer. Ainsi naquit la guerre électronique moderne et l'espionnage des signaux. À la tête de ce labo se trouvait le professeur d'ingénierie de Stanford Fred Terman qui, après la deuxième guerre mondiale, a engagé onze membres de ce labo pour créer le Labo de Recherche Électronique de Stanford (ERL), qui recevait des financements de l'armée. Stanford avait aussi

1 Serveurs de stockage délocalisés.

2 « Hacking For Defense In Silicon Valley », steveblank.com, 31 mars 2015.

un Labo d'Électronique Appliquée (AEL) qui faisait des recherches classées secrètes dans le domaine du brouillage et de l'espionnage électronique pour l'armée.

En fait, les recherches de l'AEL ont grandement contribué à la guerre US au Vietnam. Cela a fait de ce labo une cible pour les manifestants étudiants contre la guerre qui ont occupé le labo en avril 1969 et exigé la fin des recherches classées secrètes à Stanford. Après près d'un an de conférences, de manifestations et de violents affrontements avec la police, Stanford a effectivement supprimé ces recherches liées à la guerre.

« Don't be evil », Google

L'année dernière [en 2013], les premiers documents transmis par Snowden ont révélé que Google, Facebook, Yahoo!, et d'autres compagnies donnaient à la NSA l'accès aux données des usagers par le biais du programme PRISM. Toutes ces compagnies ont nié et se sont publiquement opposées à la surveillance du gouvernement. Néanmoins, Jason Leopold d'*Al Jazeera America* a obtenu, *via* une requête FOIA (Freedom Of Information Act), deux séries de courriels entre l'ancien directeur de la NSA, Keith Alexander, et des cadres de Google, Sergey Brin et Eric Schmidt. D'après Leopold, ces communications suggèrent « des relations de travail entre certaines firmes technologiques et le gouvernement US bien plus commodes que ce que laissaient entendre les huiles de la Silicon Valley » et que « toute cette coopération n'était pas menée sous pression. » Dans les courriels, Alexander et les cadres de Google s'entretiennent à propos du partage d'informations dans l'intérêt de la sécurité nationale.

Mais PRISM n'est que la partie émergée de l'iceberg. Plusieurs compagnies sont intimement liées avec les services de renseignement, l'armée et ses fournisseurs. Google en est le parfait exemple.
Google a signé un contrat avec l'Agence Nationale de Renseignement Géospatial (NGA) qui autorise cette dernière à utiliser Google Earth Builder. La NGA fournit des renseignements géospatiaux, *via* des images satellites et cartographiques, pour l'armée et d'autres agences comme la NSA. En fait, la NGA a permis à l'armée et à la CIA de localiser et de tuer Ben Laden. Le blog officiel de Google a annoncé que leur « travail avec la NGA marque une des premières initiatives majeures du gouvernement en matière de *cloud* géospatial, qui permettra à la NGA d'utiliser son programme pour conserver ses données. Cela permet à la NGA de customiser **Google Earth & Maps** pour fournir des cartes et des globes afin de soutenir les activités du gouvernement US, telles que : la sécurité nationale, la sécurité intérieure, la mesure et le contrôle environnemental, l'aide humanitaire, la capacité de réaction en cas de catastrophe. »

La technologie **Google Earth** « est née au sein de la communauté du renseignement, dans une firme soutenue par la CIA, Keyhole », que Google a racheté en 2004, selon le *Washington Post*.[3] Le reporter de PandoDaily,Yasha Levine, qui a beaucoup travaillé sur les liens entre Google, l'armée et le renseignement, souligne que « le produit principal de Keyhole était une application Earthviewer qui permettait aux usagers de voler et de se déplacer autour d'un globe virtuel comme s'ils étaient dans un jeu vidéo. »

La relation de Google avec la Sûreté nationale s'étend au-delà de ses contrats avec l'armée et les services de renseignement. De nombreux directeurs des relations publiques chez Google viennent de l'armée ou du renseignement, d'après un rapport de Levine.[4] Michele R. Weslander-Quaid est devenue à Google en 2011 Chef du Comité Technologie

3 Google Searches For Government Work, 28 fév. 2007.

4 « The revolving door between Google and the Department of Defense », pando.com, 23 avril 2014.

chargée des relations avec le secteur public. Avant de rejoindre Google, depuis le 11 septembre 2001, Weslander-Quaid « visitait les zones de combat en Irak et en Afghanistan pour voir sur place les besoins technologiques de l'armée. » À Google, son rôle est de rencontrer « les directeurs d'agences [militaires] pour faire le schéma des voies technologiques qu'ils veulent suivre, puis d'aider les employés de Google à comprendre ce dont ils ont besoin. » Weslander-Quaid confie au magazine *Entrepreneur* : « une grande partie de mon travail consiste à traduire le dialecte gouvernemental en jargon de la Silicon Valley et vice-versa ».

En décembre 2013, Google a racheté Boston Dynamics, une grande compagnie spécialisée en robotique et financée par l'armée. Selon *The Guardian*, « le financement de la majorité de leurs robots les plus avancés provient de sources militaires, dont les fonds de l'Agence pour les Projets de Recherche Avancée pour la Défense (DARPA), de l'armée, de la Navy et des marines. »[5] Certains de ces projets comprennent BigDog, Legged Squad Support System (LS3), Cheetah, WildCat et Atlas qui sont tous des robots ambulants et autonomes. Atlas est humanoïde, tandis que les autres ressemblent à des animaux quadrupèdes.

Militarisme high-tech

Amazon a récemment développé un système de *cloud* d'une valeur de 600 millions de dollars pour la CIA ainsi que l'ensemble des 17 agences de renseignements. Amazon et la CIA n'ont quasi rien révélé des capacités du système.

La technologie de la Silicon Valley a de nombreuses applications sur le champ de bataille, l'armée US l'a remarqué. Depuis le début de la guerre contre le terrorisme mondial, l'armée a, entre autres, des besoins grandissants en termes d'espionnage high-tech. « L'un des défis clefs pour l'armée est de fournir les capacités d'analyser l'énorme quantité de données collectées », note un rapport du GAO [organisme du Congrès des États-Unis qui contrôle les comptes publics]. La prolifération des drones, les opérations anti-insurrectionnelles, les systèmes sophistiqués de renseignement-surveillance-reconnaissance (ISR) ainsi que les nouvelles technologies et capteurs ont changé la manière d'utiliser l'espionnage dans les campagnes anti-insurrectionnelles d'Irak et d'Afghanistan ou les opérations anti-terroristes au Pakistan, en Somalie au Yémen et dans les autres pays.

Les guerres irrégulières contre les groupes insurgés et terroristes présentent deux problèmes – trouver les ennemis et les tuer. Parce que ces groupes savent se mêler à la population locale et souvent ils en font partie. Les armes robotiques, tels que les drones, offrent « une solution asymétrique à un problème asymétrique », selon un cadre de Foster-Miller cité dans le livre de P.W. Singer *Wired for War* [*Câblé pour le Combat*]. Les drones peuvent rester longtemps en vol stationnaire au-dessus d'un territoire et frapper une cible sur commande sans mettre les troupes américaines en danger, ce qui les rend très attrayants.

Aussi, l'armée US et les agences de renseignements comptent de plus en plus sur l'espionnage des signaux pour résoudre le problème. C'est un moyen de contrôler les signaux électroniques comme les appels téléphoniques ou radio, les e-mails, les signaux radars, etc. Les analystes ou les troupes sur le terrain collectent et analysent les communications électroniques et les données géospatiales des adversaires pour les localiser, établir un schéma de leur comportement et procéder à leur élimination. (...)

L'espionnage des signaux au service du programme d'assassinats extrajudiciaires des

5 « What is Boston Dynamics and why does Google want robots ? », 17 déc. 2013.

États-Unis est actuellement un élément majeur de la guerre contre le terrorisme international. Ce programme d'assassinats extrajudiciaires a commencé sous Bush afin de tuer partout dans le monde les personnes suspectées de terrorisme sans aucune forme de procès. Néanmoins, comme Bush se concentrait sur l'occupation massive de l'Irak et de l'Afghanistan, on a moins insisté sur le programme d'assassinats.

Le gouvernement Obama a continué la guerre contre le terrorisme mais a largement diminué les occupations à grande échelle pour mettre l'accent sur les frappes des drones de la CIA/JSOC, les attaques aériennes, les missiles téléguidés, les mercenaires et les forces d'opérations spéciales contre les terroristes soupçonnés. Obama a poursuivi et étendu le programme d'assassinats de Bush, en comptant sur les drones et les forces d'opérations spéciales pour faire le boulot. D'après le Bureau du Journalisme d'Investigation (BIJ), **les frappes des drones U.S. et autres assauts furtifs ont fait près de 3 000 à 4 800 morts, dont 500 à 1 000 civils, au Pakistan, au Yémen et en Somalie.** Pendant cinq années du gouvernement Obama, plus de 2 400 personnes ont été tuées par les drones U.S. **La plupart des victimes de ces frappes sont des civils ou des troufions et, au Pakistan, seuls 2 % étaient des militants de premier ordre.** Les communautés vivant sous la menace des drones sont régulièrement terrorisées et traumatisées par ces engins. Les cibles des drones sont repérées grâce à l'analyse des métadonnées et à la localisation de la carte SIM du portable d'un des terroristes suspectés, d'après un rapport de *The Intercept*. Ces renseignements sont fournis par la NSA et transmis à la CIA ou à la JSOC qui met à exécution le bombardement par les drones. Cependant, il est très courant pour les gens au Yémen ou au Pakistan de détenir de multiples cartes SIM, de donner leurs téléphones à des proches ou à des amis, et pour les groupes comme les Talibans de distribuer aléatoirement des cartes SIM parmi leurs combattants pour brouiller les pistes.

La proposition de budget 2015 de la Défense demandait 495,6 milliards de dollars, soit 0,4 milliards de moins que l'année précédente. Il diminuait les effectifs de l'armée à près de 440 000 soldats depuis le pic post-11 septembre élevé à 570 000. Mais il assurait de l'argent – 5,1 milliards de dollars – pour la cyberguerre et les forces d'opérations spéciales, et donnait 7,7 milliards à SOCOM (Commandement des opérations spéciales), une augmentation de 10 % depuis l'année précédente, et un personnel de 69 700 employés. Ainsi, ce type d'opérations a de fortes chances de continuer.

Comme les États-Unis mettent l'accent sur la cyberguerre, les opérations spéciales, les drones, les formes d'espionnage électronique ainsi que d'autres tactiques de combat irrégulières pour être en guerre perpétuelle, des technologies sophistiqués sont forcément nécessaires. La Silicon Valley est donc l'industrie numéro un pour réaliser les objectifs de la Sûreté de l'État.

Adam Hudson est journaliste, écrivain et photographe.
AlterNet, 19 août 2014

Traduction :
Oscar pour *Hors-sol*