À qui iront les clés de la ://Surveillance ?

Parmi les interrogations nombreuses et inquiètes qui ont accompagné l'élection du nouveau président des USA, nous retenons aujourd'hui la question de la maîtrise des armes les plus dangereuses dont va disposer l'exécutif. On pense bien sûr à l'arme nucléaire et au danger de son usage inconsidéré, mais une actualité tout aussi préoccupante nous invite à nous demander avec Cory Doctorow quelles conséquences la machine industrielle de la surveillance étatique peut avoir sur nos libertés, si elle tombe aux mains de… [mettre ici le nom de toute personnalité politique dont on peut redouter l'autoritarisme].

Cory Doctorow, qui est Canadien, réagit ici à la situation nord-américaine, mais la surveillance étatique est planétaire et nous sommes en France assez lourdement pourvus en outils de surveillance générale pour éprouver quelques inquiétudes : que deviendront par exemple le fichier TES (voir ce billet de Korben) et l'état d'urgence indéfiniment prolongé que veut imposer M. Cazeneuve si un gouvernement autoritaire accède au pouvoir bientôt ?

Au risque réel Doctorow répond par la nécessité de lutter avec nos armes, celles d'Internet. Cela suffira-t-il ?

On a donné à un cinglé les clés de la surveillance d'État

par Cory Doctorow

Article original *A madman has been given the keys to the surveillance state*

Traduction Framalang : Goofy, Framasky, Diane

Cory Doctorow par Jonathan Worth (CC-BY-SA)

Quand le *Patriot Act* a été promulgué aux USA le 26 octobre 2001, il a fait disparaître un grand nombre des contrepouvoirs vitaux qui s'interposaient entre le peuple américain et son gouvernement. Alors que les partisans de Bush applaudissaient le pouvoir sans précédent que leurs représentants à Washington détenaient désormais, les militants des libertés civiles les avertissaient : « Votre président vient de créer une arme qui sera utilisée par tous ceux qui le suivront ».

Lorsque les démocrates ont pris la Maison-Blanche en 2008, les Américains de droite ont tardé à se rendre compte qu'une nouvelle administration qui ne s'appuyait pas sur eux pour exercer son pouvoir avait la possibilité de surveiller tous leurs mouvements, pouvait pister toutes leurs communications, pouvait les soumettre à une détention sans mandat dans des « zones frontalières » qui couvraient la majeure partie de la population américaine, pouvaient saisir leurs biens sans les accuser d'aucun crime, et ils ont commencé à s'inquiéter sérieusement.

Lorsque l'administration Obama a doublé le programme Bush de surveillance de masse, en lui ajoutant de lois secrètes et une liste d'Américains et d'étrangers qui pourraient être carrément assassinés en toute impunité n'importe où dans le monde, ses partisans démocrates n'ont pas accepté d'entendre la moindre critique. Obama était un politicien expérimenté, le

père tranquille de l'Amérique, un type avec tant d'équanimité qu'il avait besoin d'un interprète pour traduire sa colère. Il n'allait pas abuser de cette autorité.

Les sept années de G.W. Bush après le 11 Septembre nous ont donné les bases d'un État de surveillance auquel il manquait un fou dangereux pour devenir totalitaire. Ensuite, huit ans après la mise en œuvre concrète de cet État de surveillance, Obama a indiqué aux administrateurs compétents et aux divers intervenants – police locale, partenaires internationaux, entrepreneurs militaires et industriels avec de gros budgets de lobbying – que cette surveillance doit se maintenir indéfiniment.

Aujourd'hui, c'est à un cinglé qu'on a donné le contrôle d'un arsenal de surveillance qui inclut l'autorité légale pour nous espionner tous, tout le temps ; des offres commerciales des monopoles des télécoms qui transforment les dépenses d'un gouvernement impopulaire en affaires rentables avec de l'argent comptant qui servira au lobbying pour élargir leur clientèle ; et un stock de vulnérabilités technologiques mortelles dans les outils dont nous dépendons, que l'Amérique a transformés en armes pour attaquer ses ennemis, même si cela implique de laisser les Américains sans défense contre les criminels, les harceleurs nihilistes, l'espionnage d'États étrangers et l'espionnage industriel.

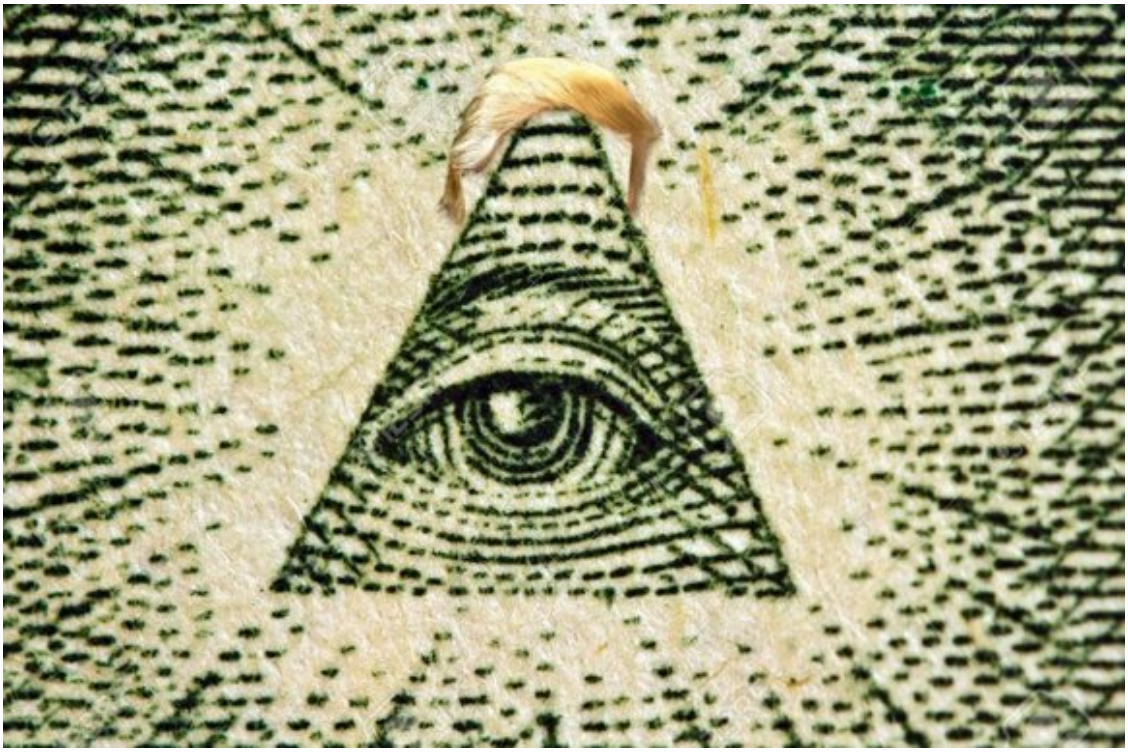

image : http://www.trumpshair.com/

Le Royaume-Uni est sur le point d'adopter une loi de surveillance qui éclipse tous les pouvoirs de surveillance de Bush et Obama. Le cyber-arsenal que Theresa May veut déchaîner sur le monde ne permettra pas seulement de vous pister en temps réel avec un degré d'intrusion qui ne peut pas être surestimé, il va également amasser des stocks énormes de données de ce suivi qui seront inévitablement fuitées, à la fois publiquement – pensez au piratage de Sony – et en privé, ce que nous découvrirons seulement des années après les faits, quand nous verrons que des escrocs minables ont exploité nos moments de chagrin et de détresse les plus privés pour en faire leur profit.

Le dernier gouvernement canadien a adopté un projet de loi de surveillance qu'on pourrait facilement qualifier de *fanfiction* du *Patriot Act*. Le gouvernement actuel – dirigé par un homme charismatique auquel beaucoup font confiance pour prendre les bonnes décisions – a voté pour elle, parce que ses membres ne voulaient pas être considérés comme « mous sur le terrorisme » à la veille de l'élection, mais ils ont promis de régler la question plus tard. Jusqu'à présent, ils n'ont strictement

rien fait du tout, et ils n'ont pas de feuille de route pour faire quoi que ce soit qui pourrait transformer cette épée en un soc de charrue[1]. Ce qui est particulier avec les pouvoirs que donne la surveillance, c'est qu'ils sont terriblement jouissifs. Une fois que vous en disposez, ils sont si pratiques qu'il est très difficile de les jeter dans les poubelles de l'Histoire.

Le gouvernement allemand de Mme Merkel – elle-même est hantée par ses souvenirs personnels d'enfance sous la surveillance intrusive des espions de la Stasi – a été scandalisé d'apprendre que le gouvernement des USA enregistrait les conversations téléphoniques de la Chancelière elle-même. Mais en fin de compte, Merkel a conclu un accord entre ses espions et leurs homologues américains et elle a officialisé le complexe industriel de surveillance. L'Allemagne est maintenant à deux doigts d'un gouvernement néo-nazi d'extrême-droite qui pourrait s'installer au milieu de la toile que Merkel a permis à ses services secrets de tisser dans tous les coins de son pays.

Après les terribles attaques de Paris, François Hollande a renié sa promesse de démantèlement de la surveillance française. Il l'a plutôt radicalement étendue, créant une arme immortelle et pluripotente pour espionner et contrôler le peuple français. Hollande est sur le point de perdre le contrôle du gouvernement français au bénéfice des néofascistes de Marine Le Pen, cheffe héréditaire d'une tribu de racistes vicieux et autoritaires.

Les mouvements politiques vont et viennent, mais les autorités institutionnelles demeurent. Les militants des partis ont offert une couverture politique à leurs leaders pendant qu'ils créaient tranquillement les conditions du fascisme clé en mains. Maintenant nous sommes à un clic du totalitarisme.

Il n'est pas trop tard.

Démanteler la surveillance d'État ne sera pas facile mais les choses importantes le sont rarement. Des organisations comme l'EFF (USA), Openmedia (Canada), la Quadrature du Net (France) et l'Open Rights Group ont mené cette bataille depuis des années, longtemps avant que la plupart d'entre nous ne prenne conscience du danger. Leur temps est maintenant : le moment où le danger est visible mais que le mal n'est pas irréversible. C'est le moment où jamais.

Les quatre ans à venir apporteront des batailles bien plus urgentes que l'avenir d'Internet : des batailles sur le droit des femmes à disposer de leur corps ; sur les meurtres racistes de la police et l'incarcération de masse, sur les déportations de masse et les camps de concentration ; sur la discrimination selon le genre et l'homophobie ; sur l'accès aux premières nécessités, depuis l'alimentation jusqu'au logement, en passant par la couverture maladie.

Chacune de ces batailles sera gagnée ou perdue en utilisant Internet.

Nous manquons de munitions, de forces vives, nous sommes trop peu nombreux et n'avons pas de plan, mais nous pouvons tout de même gagner. Internet donne l'avantage à la guerre asymétrique, là où le pouvoir brut et l'argent peuvent être contrés par des tactiques novatrices et une opposition agile.

Tor, Signal,l'identification à 2 facteurs, un VPN… des armes pour s'opposer à Trump ?

S’il nous faut remporter la victoire dans la lutte pour les droits humains et la dignité humaine, nous devons avoir pour arme un Internet libre, ouvert et équitable. Ça commence maintenant. Ça commence avec la prise de conscience suivante : nous ne pouvons pas nous permettre de créer des armes et des pouvoirs juste pour « notre camp » en croyant que l’autre camp, celui des « méchants », ne voudra pas s’en emparer. Nous avons chargé un fusil et l’avons mis entre les mains d’un cinglé. Engageons-nous à ne plus jamais le faire.

Nous continuons le combat.

À lire aussi sur le même sujet :

- How to Trump-Proof Your Electronic Communications

Note

(1) Dans la Bible, « De leurs glaives ils forgeront des houes, Et de leurs lances des serpes … » (Ésaïe 2:4). L’idée est bien sûr de convertir les armes de la guerre en outils pour la paix.