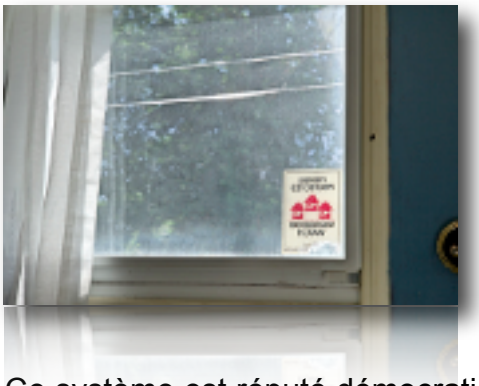
par Evgeny Morozov,
Traduction depuis l'anglais : Olivier Cyran
15 mai 2017

Cyber-insécurité

La rançon et la rente

La récente contamination par le virus "WannaCry" [1] de centaines de milliers d'ordinateurs — dont ceux des hôpitaux britanniques, d'opérateurs télécoms et autres entreprises du monde entier —, ne doit pas être balayée d'un revers de la main comme l'énième arnaque de quelques cybercriminels. Les assaillants ont utilisé des failles découvertes par les agences de sécurité américaines pour assurer leur propres missions de cyber-guerre. Dès lors, il n'est plus possible d'ignorer cette réalité dérangeante : la nature de plus en plus féodale du monde de la cyber-sécurité — que l'on peut résumer par cette alternative : être rançonné ou disparaître —, est une conséquence de l'épuisement des idéaux du capitalisme démocratique sous l'effet de la surveillance permanente.



Backdoor - cc Snapshot Heaven

Le capitalisme démocratique, cette curiosité qui nous a promis la fin de l'histoire et se targue aujourd'hui d'être le seul rempart à l'extrême droite, tire sa légitimité politique d'une distribution des rôles bien établie entre gouvernements et entreprises : aux premiers le soin de réguler les seconds, afin de protéger le consommateur contre les effets ponctuellement indésirables d'une activité par ailleurs si pleinement bénéfique.

Ce système est réputé démocratique car les gouvernements sont élus et révocables par le peuple ; il est capitaliste parce que les entreprises obéissent à une logique de compétition qui valorise l'efficacité, l'innovation et l'expansion sans limites. Une logique dont l'inclination à la destruction créative de toute chose peut produire des résultats toxiques, raison pour laquelle nous avons besoin de la tutelle bienveillante des gouvernements. C'est du moins ce que proclame le consensus qui règne au centre-gauche et au centre-droit du spectre politique

➤ lire "État et Silicon Valley, une servitude volontaire".

Les questions relatives à la guerre et à la sécurité — ainsi que les impératifs existentiels qu'elles imposent aux démocraties — ont toujours confronté ce schéma à des problèmes épineux, comme en témoignent les inquiétudes à propos du complexe militaro-industriel exprimées dans l'histoire par tant d'hommes politiques vieillissants. Les garanties démocratiques s'affaiblissent à mesure que les gouvernements resserrent leur contrôle sur les flux d'informations, verrouillent la confidentialité de

[1] Le logiciel malveillant, baptisé "Wanna Cry" ou "Wanna Crypt" est un "rançongiciel" qui, après s'être introduit dans un système informatique, en chiffre les fichiers (les "crypte") avant d'exiger une rançon pour les rendre à nouveau accessibles à leurs propriétaires.

leurs échanges internes et renforcent leurs activités de surveillance sans réels garde-fous ni contre-pouvoirs. Face à ces pratiques, la parade la plus courante consiste à dénoncer l'opacité d'un "État profond" ("deep state") traître à ses principes car n'ayant plus de comptes à rendre. À en croire les critiques, il suffirait d'un éventail de mesures légales visant à restaurer des règles de transparence et de respect de la vie privée pour que l'État recouvre ses vertus d'origine. En somme, nous pourrions parfaitement ignorer la part capitaliste du "capitalisme démocratique" et nous en sortir en tirant la bride aux agences de renseignement.

➤ Lire aussi Camille François, "Penser la cyberpaix", *Le Monde diplomatique*, avril 2016.

Hélas, le monde de 2017 ne se laisse pas aisément ranger dans des compartiments aussi étroits. Ne prenons qu'un seul exemple, celui de la cyber-sécurité. On le sait, des pays voyous s'appliquent à hacker les serveurs de leurs adversaires en Europe de l'Ouest et en Amérique du Nord. On sait également que des groupes de hackers privés, agissant pour des raisons commerciales ou politiques, causent des torts considérables à leurs cibles. Rien de tout cela n'égratigne le mythe fondateur du capitalisme démocratique, à savoir son rôle protecteur face aux dérives les plus extrêmes du monde de l'argent — au contraire, ces nouveaux dangers consolident plutôt le mythe. Ce qui le menace, en revanche, c'est la prise de conscience que les gouvernements démocratiques, via leurs agences de renseignement, creusent eux-mêmes des failles dans nos réseaux de communication, piratant sans vergogne nos téléviseurs connectés ou nos systèmes d'exploitation. La divulgation par Wikileaks des techniques de *hacking* de la CIA a donné récemment un nouvel aperçu du phénomène.

Certains diront que l'État nous espionne pour de nobles motifs : afin de repérer les signes avant-coureurs d'opérations terroristes, de suivre à la trace des réseaux criminels, de déjouer des complots sophistiqués. Quelles que soient les raisons invoquées, nous ne devrions cependant pas perdre de vue les retombées politiques plus larges produites par les nouveaux pouvoirs d'intrusion des pouvoirs publics.

Il y a d'abord le fait que l'expansion (ou même la seule conservation) des capacités de surveillance des États présuppose une insécurité structurelle permanente de nos réseaux de communication. Laquelle, en retour, fait le jeu non seulement des gouvernements démocratiques, mais aussi de toutes les autres officines de *hacking*, qu'elles opèrent pour des pays voyous ou des intérêts privés.

Or, une fois structurelle, l'insécurité n'appelle pas plus de sécurité, mais plus d'assurance. C'est la raison pour laquelle la cyber-assurance est devenue l'un des segments les plus prometteurs du marché de l'assurance. Même des secteurs comme celui de l'industrie manufacturière, elle aussi de plus en plus connectée et interconnectée, dépensent des sommes extravagantes pour s'assurer contre les cyber-attaques.

L'expansion des capacités de surveillance des États présuppose une insécurité structurelle permanente de nos réseaux de communication. Or, une fois structurelle, l'insécurité n'appelle pas plus de sécurité, mais plus d'assurance

Dans ce domaine-là comme dans les autres, l'assurance reste d'abord une affaire de rentiers qui excellent dans l'art de majorer les primes perçues pour leurs services. La seule nouveauté, ici, tient au fait que les risques couverts par cette nouvelle classe de rentiers découlent en bonne partie — pour ne pas dire essentiellement — de l'action des gouvernements. On en arrive à un point où la logique du capitalisme démocratique ne consiste plus à amortir les dégâts causés par le secteur

privé, mais au contraire à les surpasser par ses propres agissements toxiques — dont les compagnies d'assurance pourront ensuite tirer profit de manière plus ou moins nocive, selon le jugement que l'on porte sur la nature parasitaire de leur activité économique.

La deuxième conséquence de l'extension sans fin de l'appareil de surveillance réside dans les dommages qu'elle occasionne aux entreprises plus petites et aux organisations à but non lucratif, sans parler des individus. Que l'on songe à la vision utopique que nous chérissions naguère, celle d'un monde digital où nous contrôlerions nous-mêmes nos serveurs de messagerie électronique et même, petit à petit, la mise en œuvre de notre propre conception d'un foyer connecté. Eh bien, aujourd'hui, c'est à nos risques et périls que nous tentons de conquérir un peu d'autonomie. Compte tenu de la sophistication croissante des cyber-attaques — destinées tout autant à pirater des données qu'à noyer les cibles en générant du faux trafic —, il n'échappe plus à personne que les seuls acteurs capables de défendre les usagers — les particuliers comme les entreprises — sont les grandes compagnies technologiques telles que *Google, Apple et Microsoft*. Là encore, il s'agit d'une violation frontale des prémices du capitalisme démocratique : le citoyen est invité à se chercher une protection chez les mastodontes du privé et non plus auprès de son gouvernement — contre les intrusions duquel il s'agit précisément de se protéger.

Quand l'industrie du *spam* et du *hacking* utilise le dernier cri de l'intelligence artificielle, c'en est fini de l'espoir qu'un acteur plus petit puisse encore rivaliser avec les géants de la *"tech"* qui profitent de l'insécurité structurelle créée par les gouvernements pour bétonner un peu plus leur statut de quasi-monopole. Le capitalisme démocratique est déjà devenu un capitalisme monopolistique, et c'est encore plus vrai dans sa version digitale. Que les grandes compagnies de la Silicon Valley puissent être soumises aux principes classiques de la concurrence capitaliste paraît une idée hautement saugrenue : il n'existe pas d'entrepôt assez grand pour héberger la *start-up* qui battra *Google* — pas avec les trésors de données personnelles et d'intelligence artificielle dont celle-ci regorge.

➤ lire aussi Finn Brunton, "Une histoire du *spam*", *Le Monde diplomatique*, mars 2014.

Ce nouveau compromis post-démocratique soulève un autre problème : en présentant la cyber-insécurité comme une catastrophe quasi naturelle, il délégitime le rôle qui incombe à la loi et à la politique d'arbitrer les conflits entre citoyens et corporations. Face au risque d'une inondation ou d'un tremblement de terre, il peut certes paraître imprudent de se fier à la seule puissance des pouvoirs publics : de ce point de vue, contracter une assurance n'est pas absurde. Mais cela ne doit pas nous empêcher de réclamer des normes plus exigeantes, par exemple en matière de construction, afin de minimiser les dégâts éventuels causés par un désastre climatique. Or le monde de la cyber-sécurité échappe totalement à cette logique de bon sens. Imagine-t-on un gouvernement recruter un groupe de saboteurs surpayés et sur-diplômés dans le but de démolir les défenses antisismiques de nos maisons, ne nous laissant d'autre choix que de faire appel au secteur privé pour sécuriser nos biens, que ce soit sous forme de travaux de consolidation ou de polices d'assurance ? Tel est pourtant le scénario en vigueur dans le domaine de la cyber-sécurité. La seule différence, c'est que les sinistres auxquels nous sommes confrontés sont d'origine presque entièrement humaine et peuvent donc être évités.

Imagine-t-on un gouvernement recruter un groupe de saboteurs dans le but de démolir les défenses antisismiques de nos maisons, ne nous laissant d'autre choix que de faire appel au secteur privé pour sécuriser nos biens ?

Il n’est pas inconcevable que, devant l’évidence des périls qui nous guettent, les gouvernements reconnaissent la nécessité de renforcer les lois sur la protection de la vie privée. Cependant, nous savons bien à quoi aboutirait une concession rhétorique de cette nature : l’envoi de saboteurs plus nombreux, équipés d’armes encore plus redoutables, pour affaiblir encore nos défenses.

Qui, dans ces conditions, miserait sur les protections de la loi et de la politique plutôt que sur celles promises par les sirènes du marché, aussi trompeuses et coûteuses soient-elles ?

La cyber-sécurité n’est qu’un exemple parmi d’autres de la crise de légitimité qui ronge le capitalisme démocratique et de l’état moribond des partis politiques qui ont assuré son règne pendant si longtemps. Rien d’étonnant à ce que les formations sociales-démocrates s’effondrent dans divers pays européens : elles défendent un système qui ne fonctionne plus.

Evgeny Morozov

➤ Lire Amaëlle Guitton, "Ce que l’on sait des cyberattaques visant plusieurs dizaines de pays", *Libération,* 13 mai 2017 et Jean-Marc Manach, ""WannaCry" n’est pas une cyberattaque, mais une escroquerie, Slate.fr, 15 mai 2017.