À bâbord !
Revue sociale et politique

Les Crypto Wars

Anne-Sophie Letellier

Numéro 85, automne 2020

URI : https://id.erudit.org/iderudit/95266ac

Aller au sommaire du numéro

Éditeur(s)

Revue À bâbord !

ISSN

1710-209X (imprimé)
1710-2103 (numérique)

Découvrir la revue

Citer cet article

Letellier, A.-S. (2020). Les Crypto Wars. *À bâbord !*, (85), 22–23.

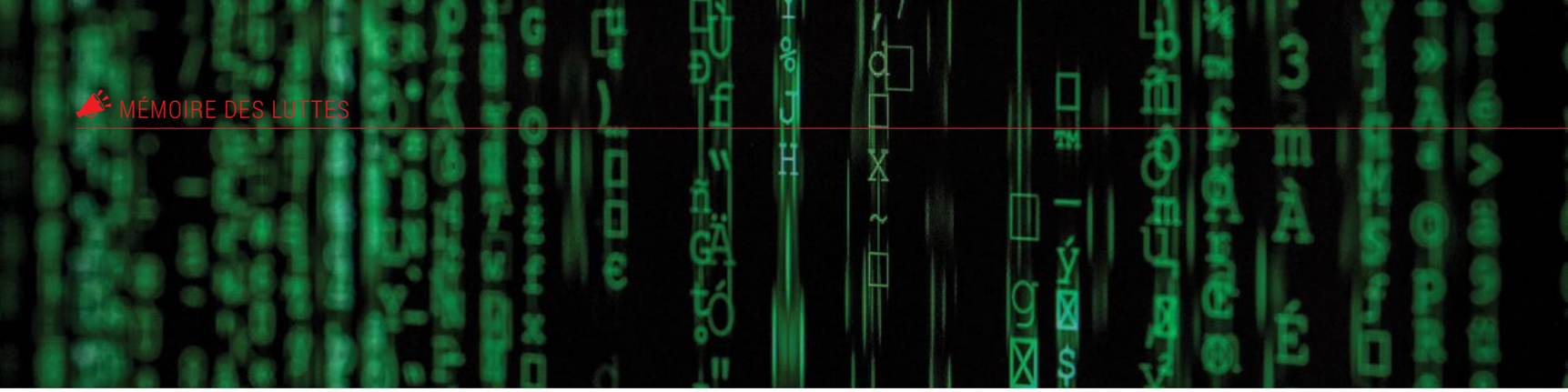

Image : Markus Spiske.

LES *CRYPTO WARS*

Anne-Sophie Letellier, candidate au doctorat en communication, UQAM

La cryptographie fait partie de nos activités quotidiennes. Si nous sommes capables de naviguer sur le Web sans être constamment exposés à des virus ou logiciels malveillants, effectuer des transactions bancaires sans crainte de fraude, ou encore échanger des communications privées avec des collègues ou ami·e·s, c'est grâce à l'implantation de systèmes cryptographiques robustes.

Ceux-ci permettent à la fois de chiffrer[1] ainsi que d'authentifier et d'assurer l'intégrité de l'information qui transite sur les réseaux numériques. Sans les systèmes cryptographiques robustes qui sont implantés dans les services et appareils que nous utilisons, le Web commercial ne pourrait exister, puisque les fraudes seraient monnaie courante, les fuites de données seraient exponentiellement plus nombreuses et il serait outrageusement risqué d'utiliser un ordinateur pour une activité jugée le moindrement confidentielle.

Or, le fait que le web que nous connaissons aujourd'hui puisse protéger – même modestement – ses utilisateur·trice·s d'une variété de menaces est dû à une série de batailles juridiques et législatives durant les années 1990 : les *Crypto Wars*. Le terme *Crypto Wars* est utilisé pour décrire les luttes menées par des avocat·e·s, cryptographes, technologues et chercheur·euse·s qui avaient pour objectif d'enlever la cryptographie à l'usage exclusif de l'État et du militaire pour en faire un outil disponible à la population en général.

LA CRYPTOGRAPHIE : UNE AFFAIRE D'ÉTAT

Les systèmes cryptographiques ont historiquement été développés et utilisés par des États, et particulièrement à des fins militaires. Durant la Seconde Guerre mondiale, par exemple, beaucoup de ressources étaient allouées pour chiffrer des communications militaires entre alliés et pour analyser et déchiffrer celles des ennemis. Jusqu'au milieu des années 1970, le monopole de l'État sur la cryptographie semblait légitime puisque l'informatique et les technologies numériques n'étaient que peu répandues en dehors des sphères étatiques.

Néanmoins, avec la popularisation des ordinateurs personnels ainsi que du Web, des membres de la société civile, des chercheur·euse·s universitaires et des entreprises privées dans le domaine émergent des télécommunications se montrent de plus en plus intéressé·e·s à l'idée de sécuriser les réseaux de télécommunication et de protéger les communications privées des citoyens (*informations en transit*) ainsi que la confidentialité des informations stockées sur des serveurs d'entreprise (*information au repos*).

Jusqu'en 1990, deux tendances se développent donc en tension. D'une part, les entreprises constatent que le chiffrement est un outil essentiel pour développer de nouvelles opportunités d'affaires, et des activistes se soucient des enjeux de vie privée qui émergent alors que de plus en plus de communications transitent via les réseaux numériques. D'autre part, le gouvernement américain est préoccupé que le développement d'algorithmes de chiffrement robustes et disponibles au public nuise stratégiquement aux opérations des agences de renseignement tout en leur faisant perdre l'avantage d'avoir un accès facile aux communications électroniques des citoyens dans le cadre d'enquêtes criminelles.

Cette tension sera au cœur des *Crypto Wars* entre 1990 et 1999. Ces *Crypto Wars* se déploieront principalement sur deux fronts. D'abord autour du contrôle des normes d'exportation des logiciels et algorithmes de chiffrement et, ensuite, dans des débats concernant l'introduction de portes dérobées dans les logiciels et services numériques.

L'INTERDICTION D'EXPORTATION

Avant 1996, toute technologie mobilisant du chiffrement robuste était considérée comme une technologie à double usage[2] et donc règlementée aux États-Unis sous le International Traffic in Arms Regulation (ITAR) et listée comme des munitions. Le gouvernement opérait donc un contrôle serré sur les algorithmes de chiffrement et exigeait une licence pour leur exportation à l'étranger. La logique était simple : le fait de limiter la capacité d'exportation des algorithmes empêchait des adversaires de chiffrer leurs communications avec des algorithmes que les services de

renseignement et d'intelligence des États-Unis étaient incapables de déchiffrer.

À compter de 1995, plusieurs décident de contester cette loi devant les tribunaux. Parmi ces personnes, on compte notamment Dan Bernstein, qui avait développé un nouveau protocole cryptographique particulièrement robuste. La loi indiquait que pour publier et partager le code source en ligne, il devait non seulement obtenir une licence, mais également s'enregistrer comme *marchand d'armes*. Avec l'organisme Electronic Frontier Foundation, il entame donc une poursuite judiciaire dans laquelle il argumente que le code d'un logiciel informatique – et, par extension, les algorithmes de chiffrement – devrait être considéré comme une forme d'expression. Après plusieurs années, la Cour d'appel américaine dépose en 1999 un jugement favorable à leur la cause, stipulant que «*le code source d'un logiciel est une forme d'expression protégée par le Premier Amendement et que, par conséquent, les régulations gouvernementales empêchant sa publication étaient anticonstitutionnelles*[3]».

LES PORTES DÉROBÉES ET L'AFFAIRE DU CLIPPER CHIP

En parallèle, le second front des *Crypto Wars* consiste, pour l'État, à cadrer dans l'imaginaire populaire le chiffrement comme une *épée à double tranchant*, c'est-à-dire un outil nécessaire à la protection des communications privées des individus, mais permettant également à des criminels de dissimuler leurs activités.

Pour ce faire, le Département d'État développe le *Clipper chip*. Le *Clipper chip* est une micropuce «à la fine pointe de la technologie» destinée à être implantée dans les appareils mobiles de manière à chiffrer avec des protocoles cryptographiques robustes, mais dont le gouvernement posséderait une clé permettant aux forces de l'ordre d'avoir accès à une version déchiffrée des communications avec un mandat approprié de la Cour. Émerge alors, en 1993, le premier de nombreux débats – qui continuent à l'heure actuelle – sur la pertinence d'introduire des «portes dérobées (*backdoors*)» de la sorte dans les systèmes cryptographiques.

Le projet du *Clipper chip* est toutefois abandonné lorsqu'un informaticien, Matt Blaze, révèle une vulnérabilité sérieuse dans la sécurité de la micropuce qui permettrait – tel que l'avaient prédit les expert·e·s – à un individu motivé de déchiffrer les communications sans avoir les autorisations requises.

LES *CRYPTO WARS* AUJOURD'HUI : LE CHIFFREMENT EST UNE FRICTION, PAS UNE BARRIÈRE

Le *Clipper chip* ne sera pas la seule tentative des agences gouvernementales de d'introduire des vulnérabilités ou des portes dérobées dans les systèmes cryptographiques. Les débats perdurent à l'heure actuelle, notamment au sein de l'alliance des Five Eyes[4] dans ce que plusieurs appellent les *Crypto Wars 2.0*. Dans ces nouvelles luttes autour de la cryptographie, on met notamment de l'avant que le chiffrement de qualité facilite les opérations criminelles et terroristes. En réponse à cela, les experts persistent à dire que l'équilibre recherché dans ces débats entre le droit à la vie privée des citoyens et la sécurité nationale est un faux dilemme puisqu'il est impossible d'implanter ce type d'accès sans compromettre significativement la sécurité des systèmes. Ce n'est donc pas uniquement la *vie privée* des citoyens qui serait affectée, mais la sécurité de l'ensemble des activités qui prennent lieu sur les réseaux numériques, augmentant significativement le risque de fuites de données, de fraude, etc. Au sein des communautés d'experts, ce constat fait «*autant l'unanimité que l'existence des changements climatiques chez les scientifiques environnementaux*[5]».

Finalement, introduire des portes dérobées aurait également pour effet d'affecter et de vulnérabiliser les activités de groupes – journalistes, militant·e·s, avocat·e·s et communautés marginalisées – déjà disproportionnellement touchés par la surveillance numérique. En ce sens, que ce soit pour protéger l'ensemble des activités prenant place sur le Web ou spécifiquement celles qui sont essentielles à nos sociétés démocratiques, il s'avère impératif de continuer de développer et d'implanter des systèmes de chiffrement robustes auprès de la population en général tout en déployant des cadres juridiques et des techniques d'enquêtes qui n'affecteront pas la sécurité globale des réseaux et les droits et libertés des individus. àbi

1. Le chiffrement des communications est un processus mathématique qui utilise un algorithme (*cipher*) dans l'objectif de modifier un texte ou une information en une série de caractères incompréhensibles (*ciphertexte*). Pour ce faire, le processus de chiffrement requiert qu'une *clé* – une série de caractères uniquement accessible à l'usager·ère ou aux usage·ère·s autorisés – soit appliquée audit algorithme afin de le rendre *unique*. Le déchiffrement des communications permet de faire le chemin inverse : la clé est utilisée afin de permettre à l'algorithme de retransformer le *ciphertexte* en texte lisible.

2. Une technologie à double usage est une technologique qui comporte à la fois un usage civil et militaire, de manière similaire aux technologies nucléaires (pouvant être utilisées à la fois pour la création d'énergie et d'armement nucléaire) ou encore à certains produits chimiques.

3. Electronic Frontier Foundation, « Bernstein v. US Department of Justice ». En ligne : www.eff.org/cases/bernstein-v-us-dept-justice.

4. Alliance stratégique entre les agences de renseignement du Canada, des États-Unis, de la Nouvelle-Zélande, de la Grande-Bretagne et de l'Australie.

5. Lex Gill, Christopher Parsons et Tamir Israël, *Shining a Light on the Encryption Debate : A Canadian Field Guide*, Toronto/Ottawa, Citizen Lab/Canadian Internet Policy and Public Interest Clinic, 2018, p.106.

POUR ALLER PLUS LOIN

Sur les questions d'actualité que sont les technologies de surveillance et de traçage de contacts, écouter une intervention d'Anne-Sophie Letellier au balado Speakeasy. En ligne : linktr.ee/speakeasy.balado

Sur la sécurité numérique en général, consulter les chroniques de l'autrice, publiées dans *À bâbord !*. En ligne : www.ababord.org/+-Letellier-Anne-Sophie-+