Sociologie et sociétés

SOCIOLOGIE ET SOCIÉTÉS

Hacktivisme : les geeks montent au front
From Internet farming to weapons of the geek

Gabriella Coleman

Volume 49, Number 2, Fall 2017

URI: https://id.erudit.org/iderudit/1054280ar
DOI: https://doi.org/10.7202/1054280ar

See table of contents

Publisher(s)

Les Presses de l'Université de Montréal

ISSN

0038-030X (print)
1492-1375 (digital)

Explore this journal

Cite this article

Coleman, G. (2017). Hacktivisme : les geeks montent au front. *Sociologie et sociétés*, *49*(2), 225–250. https://doi.org/10.7202/1054280ar

Hacktivisme : les geeks montent au front

GABRIELLA COLEMAN*
Université McGill
Courriel : gabriella.coleman@mcgill.ca

Traduit de l'anglais par Catherine Ego

Les hackeurs et leurs regroupements s'imposent maintenant comme des voix incontournables de notre vie géopolitique, voix assumées et largement entendues. Naguère encore, les hackeurs, des privilégiés économiques et sociaux, étaient vus comme d'obscurs bricoleurs férus de bidouillage technique. Aujourd'hui, ils s'expriment dans les médias grand public, participent à l'élaboration de politiques et de lois, contribuent à la création et au déploiement de nouveaux outils d'intervention politique et s'engagent même parfois dans des opérations d'action directe ou de désobéissance civile si périlleuses que nombre d'entre eux se trouvent actuellement en prison ou en exil pour avoir voulu dévoiler des actes qu'ils estimaient répréhensibles. Pourquoi ? Pourquoi les hackeurs préservent-ils certains espaces d'autonomie et comment y arrivent-ils ? Quels sont les facteurs historiques, culturels et sociologiques qui ont favo-

* Gabriella Coleman est professeure associée au Département d'histoire de l'art et d'études en communication de l'Université McGill — 853, rue Sherbrooke Ouest, Montréal (Québec) H3A 0G5, Canada. Cet article a été soumis le 24 août 2015, accepté le 27 juillet 2016 et publié sous forme électronique le 22 novembre 2016.

1. Ce texte est une traduction de l'article suivant : Coleman, G. (2017), « From Internet farming to weapons of the geek », *Current Anthropology*, 2017, vol. 58, n° S15, p. S91-S102.

risé leur entrée massive dans l'arène politique ? Pourquoi un nombre non négligeable d'entre eux optent-ils même pour la désobéissance civile, au risque d'y perdre leurs privilèges ? Loin de la vénération béate autant que de l'anathème sans appel qui polarisent l'opinion publique à l'égard des hackeurs et de leur action politique, ces questions complexes appellent des réponses nuancées. Je propose dans cet article un inventaire descriptif sommaire des traits socioculturels et des conditions historiques à l'origine de l'intensification du hacktivisme politique (l'activisme politique des hackeurs) au cours des cinq dernières années.

Après avoir prononcé une allocution sur le collectif militant Anonymous, en janvier 2015, je suis allée manger avec PW, un hackeur hollandais dans la quarantaine maintenant établi au Canada. J'avais fait sa connaissance en 2002 à l'occasion de mes recherches à Amsterdam. Puisqu'il est expert en cryptographie, notre conversation s'est naturellement portée sur Edward Snowden, cet ancien contractuel du gouvernement[2] qui a révélé l'existence des programmes secrets de surveillance mis en place par la NSA[3]. D'une certaine manière, en suscitant chez les hackeurs une prise de conscience décisive et en les ralliant à la lutte contre les abus d'ingérence, l'affaire Snowden aura aidé PW dans son combat de longue date pour le droit à la protection de la vie privée. Depuis le cri d'alerte de Snowden, nombreux sont en effet les technologues qui travaillent au développement conjoint d'outils de chiffrement pour mieux protéger les renseignements personnels.

Au cours de ce même repas, j'ai demandé à PW ce qu'il pensait de la place actuelle des hackeurs dans la vie politique. Très actif dans le monde du hacking depuis son entrée dans l'âge adulte, PW n'a pas hésité une seconde : produits, comme Internet lui-même, des technologies sur lesquelles ils travaillent, les conséquences de leur action politique se concrétiseront de manière diffuse et sur une très longue période. Pour préciser son analyse, PW ajouta que les hackeurs étaient pour lui les « fermiers d'Internet ». Tout comme l'essor de l'agriculture a remodelé en profondeur les liens entre l'être humain et ses approvisionnements alimentaires, les artefacts technologiques des hackeurs et de leurs alliés technologues feront date dans l'histoire de l'humanité. Aucun hackeur individuel ni regroupement de hackeurs n'aura d'incidence réellement cruciale sur cette évolution, ajoutait PW : elle sera plutôt la somme de leurs micro-gestes, de leurs micro-interventions au sein d'immenses dynamiques déterministes alimentées par le développement technologique lui-même.

Cette explication n'était qu'une mise en contexte… PW s'est dit ensuite très surpris de constater que les hackeurs individuels et leurs regroupements (il connaît très bien la plupart d'entre eux) interviennent de plus en plus activement dans notre histoire immédiate et notre devenir géopolitique. J'étais évidemment d'accord avec lui sur ce point : depuis plusieurs années, mes recherches sur le hacktivisme confirmaient que des espaces robustes de militantisme et d'élaboration d'outils politiques existaient en

2. Des États-Unis. (NdlT)
3. *National Security Agency*, Agence nationale de sécurité des États-Unis. (NdlT)

effet de longue date (Jordan, 2008 ; Jordan et Taylor, 2004) ; ils n'avaient cependant jamais représenté que de minuscules îlots dans un océan immensément vaste.

Notre paysage actuel est tout différent. Depuis cinq ans, les hackeurs ont considérablement élargi la portée de leur action politique ; ils expriment maintenant des opinions multiples et nuancées qui vont bien au-delà du libertarisme auquel certains analystes réduisent pourtant l'essence même du hacking (Golumbia, 2013). En particulier, l'action directe et la désobéissance civile se déploient aujourd'hui sous des formes et des styles très divers, le plus souvent par le blocage de sites Web au moyen de campagnes de déni de service distribué [*Distributed Denial of Service attack,* DDoS] (Sauter, 2014) ou par la diffusion d'alertes. Ainsi, les fuites d'information peuvent émaner de personnes agissant seules (Chelsea Manning) ou de collectifs de gauche (Xnet en Espagne). D'autres engagements politiques s'expriment par le logiciel lui-même : des protocoles (BitTorrent et autres) et des plateformes de partage de fichiers (The Pirate Bay, par exemple) permettent de diffuser très largement différents biens culturels (Beyer, 2014 ; McKelvey, 2014). Les hackeurs conçoivent ces plateformes selon l'angle idéologique qu'ils privilégient, entre anarchisme et socialisme, libéralisme et libertarisme. Depuis les années 1980, les hackeurs du logiciel libre inscrivent dans les logiciels mêmes des dispositions juridiques qui réorientent nettement le droit de la propriété intellectuelle en faveur de l'accès (Coleman, 2013 ; Kelty, 2008) et qui stimulent d'autres acteurs dans leur combat pour l'accessibilité, notamment des scientifiques, des universitaires et des juristes (Delfanti, 2013). En Europe, en Amérique latine et aux États-Unis, des hackeurs anticapitalistes s'organisent en collectifs, souvent doublés d'associations anarchistes, pour offrir aux croisés de gauche engagés dans les transformations sociales systémiques des services de soutien et des outils techniques qui les aident à mieux protéger leurs données personnelles (Wolfson, 2014). Anonymous constitue maintenant l'une des incarnations de la politisation des geeks les mieux connues du grand public ; s'il n'est pas indispensable de posséder des compétences techniques particulières pour participer à son action, c'est par la médiatisation de grandes opérations de hacking audacieuses que le collectif diffuse ses messages essentiels (Coleman, 2015).

En un mot, les hackeurs ne sont plus des experts bizarres évoluant dans un monde parallèle : ils s'imposent maintenant comme des voix incontournables de notre vie géopolitique, voix assumées et largement entendues. Naguère encore, ces privilégiés étaient vus comme d'obscurs bricoleurs férus de bidouillage technique. Aujourd'hui, ils s'expriment dans les médias grand public, participent à l'élaboration de politiques et de lois, contribuent à la création et au déploiement de nouveaux outils d'intervention politique, et s'engagent même parfois dans des opérations d'action directe ou de désobéissance civile si périlleuses que nombre d'entre eux se trouvent actuellement en prison ou en exil pour avoir voulu dévoiler des actes qu'ils estimaient répréhensibles. Pourquoi ? Ce questionnement convoque des réponses multiples.

Les technologues qui occupent des emplois conventionnels en retirent des gratifications économiques comparables à celles des médecins, des avocats ou des universi-

taires. Les activistes politiques semblent pourtant bien moins nombreux dans ces trois dernières catégories professionnelles. Pourquoi les hackeurs, qui jouissent de privilèges économiques et sociaux importants, tiennent-ils à préserver certains espaces d'autonomie ? Comment y arrivent-ils ? Quels sont les facteurs historiques, culturels et sociologiques qui ont favorisé leur entrée massive dans l'arène politique ? Pourquoi un nombre non négligeable d'entre eux osent-ils même la désobéissance civile, au risque d'y perdre leurs privilèges ? Loin de la vénération béate autant que de l'anathème sans appel qui polarisent l'opinion publique à l'égard des hackeurs et de leur action politique, ces questions complexes appellent des réponses nuancées.

Cet article propose un inventaire descriptif sommaire, un récit esquissant les traits socioculturels et les conditions historiques à l'origine de l'intensification du hacktivisme politique (l'activisme politique des hackeurs) au cours des cinq dernières années. La volonté de préserver des manières indépendantes de penser, d'être et d'interagir en constitue sans aucun doute le facteur le plus déterminant. Voyons tout d'abord comment elles s'incarnent.

GENS DE MÉTIER EN MÊME TEMPS QU'ACROBATES

Pour les utilisateurs de base comme pour les technologues aguerris, l'ordinateur constitue parfois une source inépuisable de frustration. Plantage irréversible du disque dur (s'il ne possède pas de copie de sauvegarde, l'utilisateur aura souvent l'impression qu'une partie de sa vie vient de lui être arrachée par d'exécrables forces occultes) ou, moins catastrophique, blocage abrupt d'un moteur de recherche après l'ouverture inconsidérée d'une quatre-vingt-cinquième page Web… Il est rare qu'une semaine ou même un jour se passe sans qu'une défaillance informatique quelconque n'apporte son lot de contrariétés. Je me suis justement retrouvée dans cette situation fâcheuse en octobre 2015. À la fin d'une longue journée de travail, tandis que je répondais à une pluie de courriels, j'ai distraitement ouvert cette fameuse quatre-vingt-cinquième page Web… Mon écran a d'abord figé, puis il est devenu tout noir. Ensuite, mon ordinateur, qui tourne sous un système d'exploitation Linux, a redémarré. Blême, j'ai pensé que je venais probablement de perdre plusieurs heures de travail, désormais réduites à néant au fond de sombres oubliettes — ce en quoi je n'avais pas tort. Soudain, j'ai vu apparaître ceci sur mon écran :

> Oct 8 23 : 48 : 02 kernel : [27653668.999445] Out of memory : Kill process 12731 (redacted) score 318 or sacrifice child
> [*8 oct 23 : 48 : 02 noyau : [27653668.999445] Mémoire insuffisante : tuez [arrêtez] processus 12731 (red.) score 318 ou sacrifiez un enfant*]

Sacrifier un enfant ? J'ai éclaté de rire, puis j'ai photographié l'écran. Un jour, quelque part, un développeur avait introduit cette touche d'humour dans un message d'erreur système très aride par ailleurs (et probablement incompréhensible pour les néophytes)[4].

4. Un message préconisant le sacrifice d'un enfant peut sembler bien brutal, manifestement destiné à plonger dans l'horreur l'utilisateur non initié. Mais quiconque fréquente les systèmes d'exploitation Unix

Cette mésaventure m'a rappelé que derrière tout élément logiciel se profile un créateur, un auteur possédant son propre style. Lui ayant consacré tout un chapitre (Coleman, 2013), je connaissais bien l'humour des hackeurs. Néanmoins, mon humeur maussade céda le pas au ravissement : c'était la première fois que je trouvais une pépite d'humour dans une architecture technologique sans l'avoir cherchée !

Les plaisanteries de ce type illustrent un trait caractéristique important des hackeurs, comparativement aux autres technologues qui font pourtant le même genre de travail : administrateurs de systèmes, programmeurs, cryptographes, chercheurs en sécurité. Comme les hackeurs, tous ces spécialistes sont des gens de métier animés d'un idéal d'excellence (Sennett, 2009). Le hackeur s'en distingue cependant par son irrésistible penchant pour l'acrobatie, une ingéniosité virtuose extraordinairement minutieuse et parfaitement assumée. Pour mettre la main sur des technologies informatiques ou les perfectionner, les hackeurs n'utilisent pas seulement leur savoir-faire et leurs capacités techniques : ils mettent aussi en œuvre une adresse singulière, une agilité de contorsionniste souvent teintée d'irrévérence. Ainsi que l'expliquait en entrevue un hackeur spécialisé en contournement de dispositifs de sécurité : « Il faut bien comprendre… genre… viscéralement, que la technologie, c'est arbitraire. C'est un mécanisme arbitraire qui fait quelque chose de pas naturel du tout, et qui peut donc être déjoué ; enfin… dans la plupart des cas. »

Ce va-et-vient constant entre savoir-faire et agilité, entre sage respect et mépris absolu des traditions, n'est pas propre aux hackeurs ou aux technologues. De l'ingénierie à l'enseignement, du journalisme à la charpenterie, il s'observe aussi dans bien d'autres catégories professionnelles imprégnées d'un sens aigu du travail bien fait (Orr, 1996). Ainsi, les universitaires reprennent la convention à leur compte et la perpétuent en renvoyant aux travaux de leurs confrères ; mais ils s'efforcent aussi de proposer des argumentations nouvelles allant à contre-courant des écrits de leurs prédécesseurs — en renforçant au passage leur propre renommée professionnelle. La démarche des hackeurs est un peu différente : l'astuce dont ils font preuve n'est pas qu'un moyen en vue d'une fin. Elle se déploie aussi pour elle-même, et de manière très flamboyante ; leurs acrobaties ainsi que les traits qui leur sont associés — la vivacité d'esprit, la virevolte intellectuelle… — sont par ailleurs tenus en haute estime autant pour leur forme que pour leur fonction. Pour la plupart des gens de métier, par contre, cette habileté n'est qu'un instrument, un outil parmi d'autres, et qui s'utilise souvent sans éclat, de manière discrète (Collins, 2010 ; Polyani, 1967). Pour les hackeurs, la mise en scène de leur propre virtuosité constitue depuis longtemps un but explicite, une qualité prisée en elle-même et pour elle-même.

---

sait que cette injonction est exacte du point de vue technique : quand la mémoire de l'ordinateur s'avère insuffisante pour les tâches qui lui sont demandées, le noyau Linux sélectionne un processus de manière algorithmique et l'arrête en envoyant un message *Kill process* [« tuez (arrêtez) le processus »] ; dans ce cas, cette procédure s'appliquait à un sous-processus, dit « processus enfant ». S'apparentant d'une certaine manière à un art des ténèbres, la sélection du processus à sacrifier cause sa « mort » et peut alors faire perdre à l'utilisateur une partie de son travail récent pour lui redonner accès au système.

La vénération que les hackeurs portent à l'ingéniosité acrobate s'exprime notamment par l'omniprésence de l'humour dans leurs travaux — à telle enseigne que nulle ethnographie du hacking ne saurait prétendre à une certaine exhaustivité si elle fait l'impasse sur le sujet. Ce constat m'est apparu clairement lors d'un congrès de hackeurs : les membres de l'auditoire pouvaient fort bien interrompre le conférencier de leurs blagues ; ils y étaient même encouragés ! (À part chez les comédiens et les ivrognes, rares sont les gens qui oseraient ainsi défier spontanément le décorum social.) Depuis que je m'intéresse à l'humour des hackeurs, je m'aperçois qu'ils en injectent de bonnes doses dans les situations sociales, mais aussi dans les artefacts sur lesquels ils interviennent. Le monde du hacking possède ainsi une longue tradition d'insertion de petites drôleries dans le code ou la documentation ; certains dissimulent même des énigmes (qu'ils appellent des « œufs de Pâques », *Easter eggs*) dans le code pour amuser ceux et celles qui étudient leur travail. Ils peuvent aussi créer de toutes pièces des artefacts techniques, tel ce langage de programmation exotique (ou « ésotérique ») au nom ébouriffant de « BrainFuck[5] ». Depuis toujours ou presque, les hackeurs aiment s'adonner à la farce et à l'espièglerie ; le terme *hack* lui-même proviendrait d'un mot désignant un certain type de blagues (Peterson, 2011). L'humour virevoltant des hackeurs s'exprime aussi dans certaines de leurs batailles politiques dont il sera question dans cet article. (On trouvera une analyse détaillée de l'omniprésence de l'humour et de la vivacité intellectuelle des hackeurs dans Coleman, 2013 ; Goriunova, 2014, et Montfort, 2008). En valorisant l'acrobatie pour elle-même, indépendamment de son utilité concrète, les hackeurs intègrent à leur activité ludisme et légèreté. Et surtout, ils exercent leur ingéniosité en dehors de leurs strictes préoccupations techniques et la tiennent ainsi parfaitement affûtée, toujours prête à servir dans leurs grandes actions d'éclat.

Esprits libres

> *Pour amener un hackeur à faire quelque chose, c'est simple : vous lui dites que c'est impossible.*
> (Institutionalized Oppositional Defiance Disorder [un hackeur])

L'agilité de l'acrobate reposant sur l'inlassable vigilance de l'esprit critique, l'observation sans relâche de l'environnement pour y repérer les incohérences ou renverser les conventions, les hackeurs se caractérisent aussi par un antiautoritarisme tenace, qui se manifeste notamment par un scepticisme profond à l'égard des institutions et autres pouvoirs bien établis. S'il serait tentant de ne voir dans cette affirmation qu'un cliché journalistique éculé, il n'en reste pas moins que l'antiautoritarisme est profondément encodé dans l'ADN culturel du hackeur. Il s'exprime aussi bien dans ses conversations quotidiennes que dans ses manifestes, ses magazines électroniques ou ses fichiers texte.

Le désormais célébrissime texte *The Conscience of a Hacker* [« La conscience d'un hackeur »], collectivement rebaptisé *The Hacker's Manifesto* [« Le manifeste du hac-

5. Littéralement : « Baiser le cerveau » ; le terme renvoie à la fois à la masturbation intellectuelle et à la confusion mentale face à une complexité excessive, réelle ou apparente. (NdlT)

keur »], s'avère emblématique de cet éthos. Diffusé en 1986 sous la signature d'un dénommé « The Mentor », il se conclut par une provocation en forme d'aveu : « Oui, je suis un criminel. Je commets le crime d'être curieux. Je commets le crime de juger les gens d'après ce qu'ils disent et pensent, et non d'après leur allure. Je commets le crime d'être plus intelligent que vous, et vous ne me le pardonnerez jamais » (The Mentor, 1986). Cette déclaration pourrait passer pour l'expression outrée de l'aliénation d'une classe moyenne névrosée si The Mentor, quels que soient ses moyens économiques par ailleurs, ne l'avait pas rédigée en un moment aussi décisif de sa vie : « J'ai écrit ces lignes juste après mon arrestation. »

Le parcours de The Mentor n'est pas banal : contrairement à lui, la plupart des hackeurs ne sont jamais placés en état d'arrestation. Pourtant, hier comme aujourd'hui, de nombreuses incarnations du hacking regorgent d'exemples de désobéissance à des normes, des règles, parfois des lois. L'antiautoritarisme des hackeurs s'exprime directement par ces actes répétés de subversion et, ainsi qu'en témoigne le « Manifeste du hackeur », se réaffirme constamment dans le volumineux corpus des archives littéraires et politiques du hacking. La subversion constitue en effet l'une des conditions d'émergence et d'existence du hacking. À la fin des années 1950 et au début des années 1960, quand le piratage téléphonique (*freaking*[6] ; la graphie *phreaking*, contraction de *phone* [téléphone] et *freaking*, est plus courante aujourd'hui) et le hacking ont établi leurs assises culturelles et techniques, l'accès à l'équipement exigeait souvent une transgression. Les pirates téléphoniques (*phone freaks*) agissaient rarement par appât du gain ou malveillance. Cependant, puisqu'ils entraient par effraction dans des systèmes téléphoniques pour communiquer avec d'autres utilisateurs du téléphone, ils enfreignaient inévitablement des lois fédérales ou des lois des États à chacune de leurs opérations. Les premières arrestations de pirates téléphoniques eurent lieu en 1961 (Lapsley, 2013 : 59). Il faudra toutefois attendre quelques décennies encore pour que leurs cousins hackeurs subissent aussi les foudres de la loi.

Par rapport aux pirates téléphoniques, les hackeurs rattachés aux universités enfreignaient relativement peu les lois. Le cercle restreint des étudiants hackeurs inscrits par exemple à Carnegie Mellon, à la University of California de Los Angeles, à Stanford ou au MIT, contournait par contre très souvent les règles, généralement pour travailler plus longtemps sur leurs chers ordinateurs. Dans son étude sur la première génération des hackeurs du MIT, le journaliste Steven Levy évoque en ces termes la propension des hackeurs à déjouer les règlements :

> Pour un hackeur, une porte close constitue un affront ; une porte verrouillée, un véritable outrage. Tout comme ils estiment que l'information doit être acheminée de manière élégante et limpide à l'intérieur de l'ordinateur et que les logiciels doivent être diffusés sans entraves, les hackeurs croient fermement que tout un chacun devrait avoir accès aux outils et fichiers susceptibles de favoriser la quête du hacking : discerner la manière dont le monde fonctionne et l'améliorer (Levy, 2010 [1984] : 86).

6. de *freak* : dingue, bizarre, marginal (NdlT)

Étant des étudiants universitaires, ces hackeurs ne risquaient guère d'être sanctionnés. Trop jeunes pour fréquenter l'université, des préadolescents et adolescents férus d'informatique se sont toutefois « invités » dans le club informel des technologues ; certains profitaient de l'obscurité de la nuit pour s'introduire illégalement dans les locaux, une pratique qui leur a valu d'être surnommés les « rats d'ordinateur ».

Collectivisme et espaces libres

L'antiautoritarisme et l'insubordination se retrouvent dans toutes les « familles » de hackeurs, mais à des degrés divers et sous des formes variées : par exemple, certains hackeurs désobéissent aux conventions ; d'autres se délectent d'enfreindre les lois. L'ingéniosité développée par la pratique technique et l'antiautoritarisme exprimé par le contournement des règles ou la violation des lois constituent aujourd'hui les deux répertoires rhétoriques par lesquels les hackeurs se décrivent eux-mêmes.

Dans une certaine mesure, cette ingéniosité et cet antiautoritarisme devraient donner lieu à des attitudes profondément individualistes, voire antisociales. Le mythe du hackeur farouchement libertarien s'est d'ailleurs forgé à partir de ces deux traits, extirpés de leur contexte et librement extrapolés. Les hackeurs n'entretiennent pourtant pas un rapport aussi linéaire à l'individualisme. Dans la plupart des cas, ainsi que le révèle toute observation un peu assidue de leur milieu, le hacking s'avère au contraire une activité hypersocialisée. La coopération, la camaraderie, l'entraide et même l'édification de structures institutionnelles font partie intégrante du quotidien du hackeur, et ce, même pour les plus subversifs et les plus enclins à enfreindre les règles.

Ainsi que le veut le cliché, les hackeurs consomment des doses massives de caféine pour rester en tête à tête avec leur clavier jusque tard dans la nuit… Comme eux, les gens de métier œuvrent généralement seuls. Néanmoins, leur activité professionnelle présente aussi de nombreuses dimensions collectivistes. Ainsi, ces travailleurs qualifiés se rencontrent dans des espaces sociaux, par exemple des congrès ou des ateliers, pour apprendre, encadrer les débutants ou définir des normes (évolutives) de qualité (Sennett, 2009). Le hacking ne fait pas exception à ce schéma. Que les hackeurs eux-mêmes en soient conscients ou pas, toute forme de hacking repose sur de puissants liens sociaux et sur un très fort sentiment de communauté. Ces deux éléments s'appuient sur une même vénération de l'exploration technique, mais aussi sur le besoin bien pragmatique de s'assurer l'aide de ses confrères et consœurs. Les espaces sociaux stimulent considérablement les développements technologiques conjoints et, depuis toujours ou presque, les hackeurs en construisent et en fréquentent de toutes sortes : listes d'envoi, tableaux de partage d'images, référentiels de code, projets de logiciel libre, ateliers de collaboration ou de fabrication numérique (*hackerspaces* et *makerspaces*), clavardages par IRC (*Internet Relay Chat*), congrès de développeurs et de hackeurs…

Ces lieux permettent aux hackeurs de se rencontrer, de discuter et de travailler en marge des exigences et contraintes de leur emploi conventionnel. Ils constituent ce que les spécialistes des mouvements sociaux appellent des « espaces libres ». Cette définition

proposée par une sociologue éclaire utilement le concept : l'espace libre est « un lieu situé à l'intérieur d'une communauté ou d'un mouvement, soustrait au contrôle direct des groupes dominants, d'adhésion volontaire, et porteur d'une ébullition culturelle qui précède ou accompagne une mobilisation politique » (Polletta, 1999 : 1). Les spécialistes de la question s'intéressent généralement à des lieux tels que des librairies indépendantes, des points de rencontre réservés aux femmes, des bars, des regroupements de quartier, des associations de locataires ou des locaux syndicaux.

Ces espaces ne sont pas dits « libres » parce qu'ils seraient nécessairement ouverts à tous et toutes : certains le sont (par exemple, les librairies ou les salles de clavardage publiques) ; d'autres sont dotés de règles plus ou moins strictes d'accès et d'adhésion (locaux syndicaux, projets de logiciel libre). C'est plutôt leur logique d'indépendance qui leur confère leur liberté : leurs participants les gèrent de manière collective et autonome, à l'écart du contrôle direct ou même de la simple influence des valeurs et institutions économiques, politiques ou culturelles dominantes. En effet, certaines des technologies permettant l'édification d'espaces libres, par exemple IRC et les listes d'envoi, ou les BBS (babillards électroniques) à une autre époque, sont non seulement très faciles à utiliser pour les hackeurs, mais elles ouvrent aussi des zones non commerciales dans un Internet aujourd'hui presque entièrement soumis à des intérêts privés[7].

Les hackeurs « bricolent » toutes sortes de technologies de communication pouvant aussi faire office d'espaces libres. Certains sont des institutions transparentes et structurées (par exemple, les espaces de développement de logiciels libres) ; d'autres fonctionnent en réseaux excentrés, opaques et polymorphes (les espaces libres d'Anonymous). La coexistence de ces deux configurations montre bien que les espaces des hackeurs, et par conséquent, leur sociabilité, n'ont rien de monolithique. Elle contredit aussi le mythe voulant que les hackeurs seraient farouchement individualistes ou férocement opposés à tout type d'institutions.

Les hackeurs se regroupent au contraire en dizaines d'organisations structurées. Le Projet Debian constitue sans doute l'un des plus remarquables d'entre elles. Fondé en 1993, le Projet s'enorgueillit de compter un millier de membres assurant le bon fonctionnement des 25 000 éléments logiciels constitutifs d'un système d'exploitation à base Linux. Se faisant architectes de politiques, des ingénieurs techniques de Debian ont constitué le projet en une fédération s'apparentant à une guilde ou une coopérative de travailleurs. Ils ont aussi mis sur pied des procédures raffinées de vote pour la gouvernance et ont énoncé un certain nombre d'engagements et de stipulations ratifiés dans des manifestes et chartes éthiques ou juridiques. Pour entrer dans l'organisation,

7. Plusieurs différences majeures distinguent les espaces libres des hackeurs des autres. Par rapport aux espaces libres conventionnels, qui présentent des coûts de propriété ou de location assez importants, voire exorbitants dans des villes telles que New York, Londres, Paris, Vancouver ou Sydney, les espaces libres en ligne des hackeurs sont souvent très bon marché, leurs frais se résumant généralement au prix de l'accès à Internet et à la rémunération de la main-d'œuvre nécessaire pour l'entretien des systèmes. Une étude plus approfondie du sujet devrait aussi prendre en considération les qualités matérielles des logiciels, qui autorisent le déploiement de nombreux espaces libres pour les hackeurs.

les candidats doivent subir des tests qui mesurent leur connaissance des politiques techniques, des engagements juridiques et des normes éthiques du Projet (Coleman, 2013 ; O'Neil, 2009).

Debian est en quelque sorte conçu comme une société miniature ; du point de vue social, son manifeste et sa constitution ne sont d'ailleurs pas sans évoquer le 19e siècle et les Lumières. À l'inverse, Anonymous se révèle plus opaque, mais aussi plus expansif ; le collectif fonctionne de manière plus informelle, un peu comme une « scène » (Straw, 2014). Bien qu'ils soient vus de plus en plus comme des défenseurs de la justice sociale et des chantres de l'action directe, les membres d'Anonymous refusent catégoriquement de se doter d'un dénominateur idéologique commun, et plus encore d'énoncés éthiques universels comparables à ceux qui ont été ratifiés par le Projet Debian. Présent dans le monde entier et dans d'innombrables espaces technologiques (des comptes Twitter, une multitude de salles de clavardage publiques ou privées), Anonymous est une cible dynamique et mouvante. Équipes restreintes, réseaux plus vastes ou nébuleuses de comptes Twitter vaguement reliés entre eux : nombreux sont les nœuds (ressources) et collectifs de la « famille » Anonymous qui se créent, se démantèlent et se reconstituent selon des modalités différentes en quelques semaines, voire quelques mois. D'autres se maintiennent par contre plus ou moins sous la même forme depuis maintenant cinq ans. Néanmoins, la plupart de leurs opérations semblent relativement bien organisées. Par sa géographie fluctuante, Anonymous échappe quand même à toute stabilisation. Avec le fait que certains hackeurs restent très attachés au secret de leur action, au moins dans certains domaines, ces traits caractéristiques font d'Anonymous un acteur singulier (ainsi qu'une bouffée d'air frais) par sa manière même de résister à toute cartographie sociologique un peu précise, et donc, à toute catégorisation.

Alors que Debian s'appuie sur un certain nombre de règles, Anonymous est l'anti-algorithme par excellence : difficile à prévoir, difficile à contrôler. Plus qu'une solution, Anonymous est une énigme, un message crypté. Toutefois, à ces deux extrêmes du spectre comme dans chacune des configurations intermédiaires, les participants de ces groupes s'avèrent extraordinairement sociaux. Même si les membres d'Anonymous ne connaissent pas exactement l'identité de leurs interlocuteurs, à l'instar des développeurs de Debian, ils communiquent constamment avec des « collègues » dûment sélectionnés par le regroupement : pour devenir officiellement membres du projet virtuel, les candidats développeurs doivent faire vérifier leur identité cryptographique en personne par un autre développeur.

L'intervention de l'État comme catalyseur politique

Les trois aspects cruciaux de la subjectivité du hackeur que nous venons d'examiner — la valorisation de l'acrobatie, la culture de l'antiautoritarisme pleinement assumé et les relations de compagnonnage dans le travail conjoint en espaces libres — vont nous aider maintenant à mieux cerner le hackeur en tant que sujet politique. Ces traits n'expliquent pas en eux-mêmes la propension des hackeurs à passer à l'action poli-

tique. Cependant, parce qu'ils renforcent et font essaimer l'indépendance d'esprit, les communautés d'entraide et les compétences nécessaires au maintien et au perfectionnement de technologies propices à l'action et aux regroupements autonomes, ils contribuent très concrètement à l'essor des formes d'action politique qui se développent actuellement dans cette collectivité.

Ces aspects établissent la possibilité de l'action, mais ils ne lui fournissent pas de scénario, pas de problème susceptible de l'enclencher. Si le hacktivisme actuel s'intéresse de plus en plus à des préoccupations de personnes et de groupes extérieurs, les hackeurs, fondamentalement, se mobilisent surtout contre les dangers qui menacent leur propre collectivité (Coleman, 2016). Par conséquent, et cela n'a sans doute rien d'étonnant, les hackeurs se sont beaucoup politisés en réaction aux interventions massives de l'État et à l'hostilité du monde des entreprises envers eux et envers leurs technologies. En ce sens, le public hackeur constitue un bon exemple de ce que Michael Warner (2002) appelle un « contre-public » : un public qui, « dans une certaine mesure, consciemment ou non, se sait subordonné » (56). Dans notre contexte, ce terme renvoie simplement au fait que les hackeurs, leurs activités et leurs artefacts sont souvent contestés dans leur existence même par des forces étatiques bien plus puissantes qu'eux. Mais surtout, les hackeurs expriment très fortement leur position de subordination chaque fois que l'État ou le marché entreprend de les opprimer, en réagissant généralement par la riposte. De telles situations se sont déjà produites remarquablement souvent dans l'histoire pourtant très courte du hacking. Je vais maintenant en décrire quelques-unes.

Dans les années 1980, le *phreaking* cède le pas à l'exploration tous azimuts des réseaux informatiques : la culture « hackeur underground » est née. La baisse des prix des ordinateurs personnels et des modems permet à un nombre grandissant de gens de s'adonner au sport extrême de l'intrusion dans un système informatique. Elle induit aussi une multiplication des « points d'eau » [*watering holes*], les espaces libres de l'époque : les hackeurs en émergence les créent pour se regrouper, s'échanger de l'information et entreposer les fruits de leur contrebande, grâce notamment aux babillards électroniques [*Bulletin Board Systems*, BBS] et aux concentrateurs (répartiteurs) d'ordinateurs à base texte accessibles par modem et téléphone. L'essor de la culture « hackeur underground » et l'accroissement du nombre des hackeurs se traduisent également par une augmentation exponentielle de leurs actes illégaux (Dreyfus, 1997 ; Sterling, 1992). Mais surtout, de nouvelles réglementations visant spécifiquement les utilisateurs d'ordinateurs sont adoptées à l'époque pour intercepter les contrevenants, engager des poursuites contre eux et leur imposer de lourdes peines : *Computer Fraud and Abuse Act* aux États-Unis en 1986[8], *Crimes Legislation Amendment Act* en Australie en 1989, *Computer Misuse Act* au Royaume-Uni en 1990[9].

---

8. *Computer Fraud and Abuse Act*, 1986, Pub. L. n° 99-474, 100 Stat. 1213, codifiée au titre de l'amendement 18 U.S.C. §103 (1986).

9. *Computer Misuse Act*, 1990, c.18. *Crimes Legislation Amendment Act*, 1989, n° 108.

Tout au long des années 1990, les forces de l'ordre coordonnent des opérations multi-États qui ciblent les hackeurs et leurs communautés, notamment dans le but de fermer les BBS. Des accusations inventées de toutes pièces et des amendes complètement disproportionnées par rapport aux crimes invoqués leur sont infligées. Dans sa chronique des interventions menées aux États-Unis dans les années 1990, Bruce Sterling (1992) les décrit en ces termes très clairs : « …des opérations répressives bien orchestrées, un projet délibéré de frapper leurs activités [celles des hackeurs] en plein cœur pour les neutraliser, les épouvanter suffisamment pour éradiquer une bonne fois pour toutes cette pagaille de la clandestinité numérique » (104).

Sur toutes les arrestations réalisées aux États-Unis dans les années 1990, la plus scandaleuse reste sans conteste celle de Craig Neidorf. Connu dans les milieux du hacking sous le pseudonyme de « Knight Lightning », Neidorf est le cofondateur du célèbre magazine électronique *Phrack*, renommé pour ses contenus outranciers et son antiautoritarisme implacable s'exprimant notamment par de cinglantes parodies du FBI. Neidorf est d'abord condamné à 31 ans de prison pour avoir diffusé une note technique d'AT&T sur le 911, le système téléphonique national d'appels d'urgence. Il s'avère rapidement que n'importe qui peut se procurer ce document à la bibliothèque. Les accusations seront finalement abandonnées, mais au terme d'une longue et coûteuse bataille juridique. Le calvaire de Neidorf contribuera quand même à la mise sur pied de la Electronic Frontier Foundation, qui est aujourd'hui le plus grand organisme sans but lucratif de défense des libertés civiques dans la sphère numérique.

Plus tard, d'autres cas tout aussi troublants montrent que les poursuites intentées par l'État contre les hackeurs semblent bel et bien tenir de l'acharnement (Thomas, 2003). Au début des années 2000, le hackeur et pirate téléphonique Kevin Mitnick s'introduit à maintes reprises dans divers systèmes informatiques. Ces virées en ligne, incontestablement de nature criminelle, ne lui rapportent toutefois rien du point de vue financier et ne causent aucun dommage permanent. Mais parce qu'il est un « hackeur », le ministère de la Justice des États-Unis le garde pendant quatre ans en prison avant son procès, puis l'enferme huit mois en isolement. S'il est soumis à un traitement aussi sévère, c'est que les représentants des forces de l'ordre ont réussi à convaincre le juge que Mitnick pouvait « déclencher une guerre nucléaire en sifflotant dans un téléphone public[10]. »

Dans les années 1990 et 2000, les intrusions informatiques représentent la majeure partie des infractions constatées. Sur l'ensemble des hackeurs concernés, rares sont ceux qui cherchent à tirer profit de leurs « balades » illicites dans les réseaux informatiques ; plus rares encore sont ceux qui tentent d'endommager l'équipement ou les données. Le plus souvent, leur principal crime consiste à engranger des données techniques ou à escroquer les entreprises de téléphonie pour passer gratuitement les appels nécessaires à leur exploration des réseaux. Une dizaine de cas très médiatisés se retrouvent néanmoins devant les tribunaux, et suffisent pour que les journalistes

10. Cité dans Mills (2008).

évoquent des « hackeurs fous », de « véritables Hannibal Lecter de l'électronique[11] ». Stigmatisés par les tribunaux et les médias, qui les présentent comme les nouveaux bandits de grands chemins, les hackeurs se dressent encore plus vigoureusement contre l'autoritarisme et s'investissent massivement dans des campagnes qui, comme le mouvement « Free Kevin » [Liberté pour Kevin], cherchent à sensibiliser le grand public au calvaire des hackeurs incarcérés.

Seul un nombre restreint de hackeurs enfreignent ou enfreindraient la loi pour vivre des sensations fortes lors de virées en territoires interdits (et jouir ensuite du plaisir de raconter leurs exploits clandestins à leurs pairs). La plupart sont en fait des citoyens et citoyennes respectueux des lois ; certains n'éprouvent même aucune compassion envers leurs « confrères » aux prises avec des démêlés judiciaires pour être entrés par effraction dans des dispositifs de sécurité. Ils peuvent cependant passer à l'action, y compris l'action directe, si les conditions indispensables pour écrire ou diffuser des logiciels sont menacées ou si les logiciels eux-mêmes sont visés par la censure ou la criminalisation.

Tel a été le cas de Pretty Good Privacy, un logiciel public de chiffrement écrit principalement par le cryptographe Phil Zimmerman et conçu pour mieux protéger les données privées des citoyens ordinaires. En 1991, sa diffusion internationale a constitué un acte audacieux de désobéissance civile, mais aussi une infraction aux lois sur les brevets et les munitions qui, semble-t-il, protégeaient les usages militaires du chiffrement (Greenberg, 2012 ; Levy, 2001, 2010 [1984]). En 1993, l'enquête criminelle du FBI sur Zimmerman pour exportation illicite de munitions donne une nouvelle tournure à deux réflexions émergentes : l'idée, toute nouvelle à l'époque, que les logiciels devraient bénéficier des protections garanties par la liberté d'expression ; et celle, plus générale, selon laquelle la publication de logiciels peut constituer un acte de rébellion. Le sujet fait alors couler beaucoup d'encre virtuelle dans les forums en ligne. Pour défendre le cryptage public, des hackeurs traversent des frontières internationales en arborant des T-shirts sur lesquels figuraient des codes sources de chiffrement protégés par des dispositions légales. Zimmerman étant poursuivi aux États-Unis, un dispositif très ingénieux est mis en œuvre pour l'appuyer dans son combat contre les lois sur les exportations qu'il est accusé d'avoir enfreintes : en plus de diffuser le code source en ligne, les Presses du MIT publient le schéma complet du logiciel sous forme de livre, ce qui garantit la protection du Premier Amendement aux exemplaires imprimés du code vendus à l'international. Le FBI abandonnera mystérieusement toutes ses poursuites — et n'a jamais voulu s'expliquer sur ce revirement soudain.

Entre 1999 et 2001, l'État intervient de manière très musclée pour détruire DeCSS, un court programme servant à déjouer les dispositifs d'interdiction d'accès des DVD commerciaux et permettre ainsi leur utilisation sous systèmes d'exploitation Linux ou en dehors des régions qui leur sont attribuées. Cette fois, les hackeurs sont plus nom-

11. « Geraldo Rivera Browbeats Craig Neidorf », RDFRN, http://www.rdfrn.com/totse/en/hack/legalities_of_hacking/geraldo.html (page consultée le 23 juin 2015).

breux à protester. Dans la foulée de l'arrestation de Jon Johansen, un adolescent norvégien accusé d'avoir développé et diffusé le programme, des hackeurs des États-Unis ayant partagé ou publié le code sont poursuivis en vertu du *Digital Millennium Copyright Act*. Adoptée en 1998, cette loi sur la propriété intellectuelle interdit le contournement des dispositifs de protection des droits d'auteur numériques. En Europe comme en Amérique du Nord, cette opération de criminalisation suscite des protestations sans précédent chez les hackeurs, en particulier les développeurs de logiciels libres. En plus de participer à des manifestations publiques, nombreux sont ceux qui partagent le code, un acte de désobéissance civile doublé d'une provocation parfaitement assumée : ils republient DeCSS en ligne, réécrivent le programme initial en divers langages informatiques et impriment le code de DeCSS sur des T-shirts. Certains optent pour des formes de protestation encore plus acrobatiques et subtiles : le hackeur Seth Schoen (2001) réécrit mathématiquement le programme sous forme de haïku — ou plutôt, sous forme de poème épique constitué de 465 haïkus enchaînés entre eux. S'adressant aux juges chargés de se prononcer sur les poursuites, Soen défend passionnément son travail, qu'il présente comme l'alliance des « mathématiques de la controverse » et de la poésie. Son texte exhorte ses lecteurs en ces termes[12] :

> Vois comme techno-comm
> et liberté d'expression
> doivent rimer ensemble !
> Vois comme chiffres et règles,
> motifs et langages encore
> inconnus de toi
> devraient vivre libres,
> protégés par la loi
> comme paroles vitales !

Bien qu'il émane d'un auteur unique, ce poème s'inscrit parfaitement dans ce mouvement plus collectif qui réclame l'application des dispositions protégeant la liberté d'expression à l'écriture, à la diffusion et au partage des codes (Coleman, 2013).

À l'époque, tous les geeks, hackeurs, avocats des droits civiques et libertariens radicaux entendent parler de l'imbroglio juridique de DeCSS et des actions militantes qui en découlent ; l'affaire donne même naissance à ce qu'il est maintenant convenu d'appeler le « mouvement des droits numériques » (Postigo, 2012). Cependant, les

12. La version originale de ce haïku est la suivante :
Reader, see how yet
technical communicants
deserve free speech rights ;
see how numbers, rules,
patterns, languages you don't
yourself speak yet,
still should in law be
protected from suppression,
called valuable speech !

médias conventionnels en parlent à peine, et le grand public ne prend jamais la pleine mesure de ses implications. Il faudra attendre une dizaine d'années pour que les médias conventionnels s'intéressent massivement au sujet, au gré de l'émergence de personnages et de regroupements tels que WikiLeaks, Chelsea Manning, Julian Assange, Anonymous, Aaron Swartz ou Edward Snowden. Soutenus par leurs confrères hackeurs, conspués par la plupart des centres de pouvoir, ces nouveaux acteurs n'en sont pas moins aujourd'hui très largement connus du grand public en Occident.

La diffusion par WikiLeaks de la vidéo de guerre intitulée *Collateral Murder* [« Meurtre collatéral »], en avril 2010, puis celle d'innombrables câbles diplomatiques donnent une nouvelle orientation au militantisme politique des hackeurs et catapultent au passage plusieurs personnalités sur la scène internationale — notamment Chelsea Manning, à l'origine du fuitage d'information vers WikiLeaks. Dès 2011, les opérations habilement orchestrées et spectaculairement médiatiques d'Anonymous confirment que ce foisonnement soudain d'action directe et d'activité politique ne sera pas qu'un feu de paille.

À l'instar de la génération précédente, ces hackeurs s'attirent les foudres des autorités. Chelsea Manning est condamnée à 35 ans de prison militaire aux États-Unis ; Aaron Swartz se suicide après avoir été menacé d'une absurde sentence de 35 ans d'incarcération pour téléchargement d'articles universitaires. Comme de nombreux autres militants d'Anonymous, Jeremy Hammond est arrêté et incarcéré pour diverses accusations reliées au hacking. Dans certains cas, par exemple WikiLeaks et Edward Snowden, des moyens d'une ampleur inouïe sont déployés contre les hackeurs et mobilisent des forces de l'ordre sur d'immenses territoires. Acculés par les efforts concertés de plusieurs États occidentaux bien déterminés à les capturer, Julian Assange et Edward Snowden flottent actuellement dans des limbes juridiques et vivent en exil à l'ambassade de l'Équateur à Londres et en Russie, respectivement.

D'un certain point de vue au moins, ces événements bénéficient cependant d'une réception très différente de celles des incidents antérieurs. Loin de diaboliser les hackeurs en cause ou de garder le silence sur leurs déboires juridiques, les médias se font l'écho de leur situation et expriment même parfois de la sympathie à leur égard (Thorsen, Sreedharan et Allan, 2013). Les médias culturels grand public les présentent même régulièrement sous les traits de héros ou antihéros admirables. Des séries télévisées comportent ainsi des personnages de hackeurs puissants et incontournables : *Mr. Robot*, *House of Cards*, *The Good Wife*, *Homeland*… Des longs métrages leur sont consacrés (*Who Am I*). Les distinctions culturelles les plus prestigieuses de l'Occident récompensent maintenant des documentaires présentant les hackeurs sous un jour favorable ; à titre d'exemple, *Citizenfour* a valu un Academy Award à sa réalisatrice, Laura Poitras. Jusqu'ici, les opérations de répression et la reconnaissance des milieux culturels semblent plutôt grossir les rangs des hacktivistes. L'autoritarisme de l'État fait réagir les hackeurs ; sur d'autres tribunes, ces mêmes réactions leur acquièrent la faveur populaire…

En drainant vers eux une multitude de sympathisants et d'alliés, les manifestations des hackeurs et leurs luttes les plus publicisées (par exemple, les actions d'éclat de Wikileaks en faveur d'une liberté de presse radicale ou la participation d'Anonymous à tous les grands mouvements de contestation sociale de 2011) ont élargi la portée de leurs interventions à de nouvelles sphères extrêmement diverses. Aiguillonnés par ces événements exceptionnels, nombreux sont les hackeurs et leurs cousins geeks qui ont renoncé à leur frilosité ou leur indifférence politique pour s'engager pleinement dans l'organisation et l'activisme.

Hacktivismes libéraux et radicaux

Maintenant que nous avons défini les circonstances qui amènent certains hackeurs à se positionner activement et publiquement sur l'échiquier politique, intéressons-nous à la teneur et à la tonalité de leur engagement. Dans quels combats s'investissent-ils ? S'inscrivent-ils dans la continuité de tendances et traditions politiques plus larges ou s'en démarquent-ils ? Si les hackeurs ne sont pas les libertariens que l'on croit souvent, qui sont-ils ? Des anarchistes sociaux ? Des rebelles sans cause ? Des libéraux réformistes ? Ces questions donnent lieu à des réponses multiples. L'analyse des relations entre les hackeurs et la loi nous fournira néanmoins quelques pistes. Ici encore, loin du cliché de l'antiautoritarisme pur et dur, des nuances s'imposent. Après tout, le code d'un programme informatique fonctionne, à bien des égards, comme un texte de loi.

Les hackeurs n'entretiennent pas uniquement des relations d'antagonisme avec la loi ; ils l'abordent aussi sous l'angle de l'analyse et de la recherche, parfois même de la coopération. Ainsi que je l'ai montré ailleurs, l'écriture de code s'apparente au droit en tant qu'interprétation de textes produits par un système formel reposant sur des règles bien définies : ces deux activités font appel à des types de raisonnements très similaires (Coleman, 2013). Si la plupart des hackeurs n'éprouvent que du mépris à l'égard des lois iniques et des poursuites abusives dont ils sont souvent la cible, ils s'intéressent par contre de très près aux principes, dispositions et architectures juridiques, un domaine pour lequel ils possèdent d'ailleurs généralement une certaine facilité.

Les hackeurs mettent souvent leurs aptitudes juridiques au service du changement social, particulièrement pour détecter les lois qu'ils jugent mauvaises, pour les contourner ou les contester, ou encore, comme dans le cas du logiciel libre, pour les déjouer afin de continuer à produire librement. Mais leurs talents juridiques peuvent s'avérer d'une utilité encore plus grande. Bien qu'elle rende compte de la saturation du droit dans la société anglaise du 18e siècle, cette citation de l'historien E. P. Thomson pourrait tout aussi bien s'appliquer à l'Occident actuel :

> Car le droit ne restait pas bien poliment à un seul « niveau », il se retrouvait à *tous* les foutus niveaux. Il était imbriqué dans le mode de production et jusque dans les rapports productifs […], et il était en même temps présent dans la philosophie de Locke. Il s'introduisait brusquement dans des catégories étrangères, réapparaissant déguisé de pied en cap en idéologie. […] Il était une arme pour la politique, et la politique était l'une de ses armes. Il constituait une discipline académique, soumise à la rigueur de sa propre logique

> autonome. Il contribuait à la définition de l'identité des dirigeants comme des dirigés. Et, par-dessus tout, il ouvrait une arène pour la lutte des classes, dans laquelle des conceptions alternatives du droit s'affrontaient. (Thompson, 2015 : 191-192)

Pour les hackeurs, la loi est bien plus qu'une amie ou une ennemie : elle est leur réalité. Cet enchevêtrement du hacking et du droit a souvent donné lieu à des mouvements d'esquive ou d'affrontement, quoique pas toujours dans le contexte d'une lutte des classes. Les hackeurs défendent des conceptions différentes de la loi, mais ils se battent aussi pour des préceptes juridiques bien établis qui leur tiennent à cœur et qu'ils estiment avoir été corrompus. En particulier, les principes juridiques se rapportant aux libertés civiles, notamment la vie privée et la liberté d'expression, occupent une place tellement centrale dans la culture des hackeurs et dans leurs activités techniques que leur défense s'avère presque indissociable de l'essence même du hacking.

Quand il explique pourquoi il a diffusé les documents de la NSA prouvant la surveillance des moindres faits et gestes des citoyens par les gouvernements des États-Unis et de la Grande-Bretagne, Edward Snowden exprime clairement cette acculturation très forte aux libertés civiles. Réfugié dans un hôtel de Hong Kong, il déclare au journaliste Glenn Greenwald :

> Je me rappelle de ce qu'était l'Internet avant d'être surveillé. […] Des enfants d'une partie du monde pouvaient avoir une discussion d'égal à égal, où en quelque sorte on accordait un respect équivalent à leurs idées et leurs paroles, avec des experts venant d'une autre partie du monde, à n'importe quel sujet […]. C'était libre et sans retenue. Nous avons vu le ralentissement, le déclin et la mutation de ce modèle vers quelque chose où les gens modèrent leurs opinions. […] C'est devenu comme prévisible, on s'attend à être surveillés. […]. Ça limite le champ de leur exploration intellectuelle. Je préfère plutôt *risquer la prison* […] que de risquer toute limitation de ma liberté de penser […][13].

Pour Snowden, Internet doit servir à la libre pensée et à la circulation sans entraves des idées. Pour tous ceux et celles qui partagent son point de vue, la protection des libertés civiles n'est pas connexe ni complémentaire des technologies d'Internet : elle en fait partie intégrante. Snowden est un cas d'exception en ceci qu'il a pris des risques considérables pour dévoiler l'ampleur de la surveillance actuelle. Très nombreux sont toutefois les geeks qui partagent sa conception d'Internet en tant qu'« ordre moral », pour reprendre les termes de Chris Kelty (2008). L'attachement des hackeurs aux libertés civiles renvoie à leur volonté de maintenir leur propre existence en tant qu'entité. Ils constituent ainsi ce que Kelty (2000) appelle un « public récursif » — un groupe qui veille à la préservation des libertés nécessaires à la poursuite de l'action technique et culturelle qu'il définit pour lui-même.

Les hackeurs s'intéressant de près aux libertés civiles, une bonne partie de leurs opérations politiques actuelles s'inscrivent naturellement dans la droite ligne des projets libéraux ou libertariens, voire les favorisent (Loveluck, 2015). Les exemples sont

---

13. Extrait du documentaire *Citizenfour*, réalisation : Laura Poitras (2014, Toronto : Praxis). C'est moi qui souligne.

nombreux : la constitution en bonne et due forme des partis Pirate, qui aspirent à la participation politique démocratique et libérale (Beyer, 2014 ; Burkart, 2014), ou encore les fonctions de chien de garde assumées par des associations telles que le Chaos Computer Club allemand, qui travaille régulièrement avec des journalistes (Kubitschko, 2015). Forgeant divers outils pour résoudre les problèmes qui minent l'ordre politique occidental actuel, le hacking civique constitue l'expression emblématique de cet engagement libéral. S'il vise dans certains cas une amélioration des services au niveau local, il cherche aussi à faciliter l'accès aux données et aux processus dans l'optique de contraindre les gouvernements à plus de transparence et de les obliger à rendre compte de leurs actions (Schrock, 2016).

D'autres hackeurs prennent appui sur les libertés civiles pour développer une approche plus radicale par l'ouverture d'espaces d'autonomie ou d'altérité (Söderberg, 2007 ; Wark, 2004). Ainsi, les adeptes du logiciel libre peuvent bâtir des logiciels dans des contextes commerciaux ou non commerciaux sans jamais perdre la mainmise sur les produits qu'ils créent. En fustigeant et combattant la soif de renommée et la fanfaronnade, Anonymous incarne une pratique de l'égalitarisme et de la solidarité critique des mœurs actuelles (Coleman, 2015) et préserve dans de grands médias sociaux un espace essentiel pour les gens dont l'éthique n'est pas compatible avec la logique de l'image de marque individualisée (Marwick et boyd, 2011).

Les hacktivistes s'investissent aussi dans des actes de résistance plus affirmés, en rupture ou en opposition complète avec le libéralisme et le capitalisme. Se revendiquant anarchistes, socialistes ou marxistes, de nombreux hackeurs construisent des outils et des systèmes de soutien propices à l'expression de formes d'autonomie plus radicales, et s'engagent même parfois dans des projets révolutionnaires de changements systémiques (voir Juris, 2008 ; Milan, 2013 ; Wolfson, 2014). Parmi ces initiatives, Indymedia se démarque par son ampleur et sa force de frappe. Complètement à part du paysage médiatique conventionnel, ce média indépendant a été conçu par des hackeurs qui travaillaient à l'organisation des grandes manifestations entourant le sommet de l'Organisation mondiale du commerce de 1999 à Seattle. (Il a ensuite suscité dans son sillage d'innombrables projets similaires.) Ayant prévu que les médias conventionnels monopoliseraient la représentation de la contestation et en montreraient une image faussée par la simplification à outrance et les distorsions, ses créateurs ont voulu développer une architecture médiatique distincte. Reposant sur un système de gestion des contenus novateur, elle leur permettait d'intégrer des vidéos et des photos dans leurs articles en ligne — et ce, plusieurs années avant que les prétendus « experts » n'annoncent l'invention de ces fonctionnalités par des entreprises du Web 2.0 en grande pompe, et à tort. Avec ces nouveaux outils, les hackeurs voulaient permettre aux organisateurs des manifestations et autres contestataires de contourner les médias pour devenir eux-mêmes le média.

Au plus fort de son activité, l'équipe technique d'Indymedia était à l'œuvre dans toutes les régions du monde et assurait le fonctionnement de plusieurs centaines de « salles de presse ». Ces ressources matérielles ont de toute évidence favorisé le

déploiement du mouvement pour la justice sociale, non seulement dans l'espace, mais aussi dans le temps. Un réseau très serré de hackeurs révolutionnaires s'est constitué au passage et reste bien vivace aujourd'hui, alors même que cela fait des années que le mouvement altermondialiste ne respire plus que dans les livres d'histoire de la contestation.

Depuis, ce groupe de hackeurs a aussi créé une architecture technique concurrente d'Internet commercial, une structure bâtie sur le refus systématique d'épier les utilisateurs comme le font maintenant toutes les entreprises d'Internet offrant des services réputés « gratuits » (Milberry, 2014). Cette infrastructure s'appuie sur une myriade de fournisseurs d'accès indépendants, dont une bonne partie fonctionne d'ailleurs selon des principes anarchistes de consensus. Il en existe actuellement une trentaine dans le monde, et leurs noms témoignent avec éloquence de leur radicalité : cybrigade, squat.net, systemausfall.org, flag.blackened.net, hackbloc.org, mutualaid.org, riseup.net, resist.ca, entodaspartes.org, MayFirst, etc. Riseup, aux États-Unis, est le plus important de ces regroupements. Mis sur pied par certains des hackeurs à l'origine d'Indymedia, ce collectif procure des services de listes d'envoi et de courriels sécurisés à des technologues, mais aussi à des organismes de gauche dont les visées politiques n'ont souvent rien de technologique. Pour les membres de Riseup, la technologie n'est pas une fin en soi ; c'est un outil pour créer une société libre, un monde dans lequel nous pouvons tous et toutes vivre à l'abri du besoin, dans lequel règne la liberté d'expression, un monde sans oppression ni hiérarchie, un monde dans lequel le pouvoir est également partagé[14].

Ces engagements témoignent de la diversité des orientations idéologiques chez les hacktivistes : certains hackeurs ou regroupements de hackeurs s'inscrivent dans la tradition du libéralisme ; d'autres sont radicaux. Dans les deux cas, ils sont des agents de changement social. Tous les hackeurs politisés restent très attachés aux libertés civiles, mais pas pour les mêmes raisons. Pour les libéraux, les libertés civiles constituent la condition essentielle des droits individuels et de la participation à la vie politique conventionnelle (ou de l'accès, ou de la prise de parole). Pour les hackeurs radicaux, par contre, les libertés civiles (liberté d'expression, droit au respect de la vie privée, etc.) sont plutôt des tremplins permettant la mise en œuvre de projets qui favorisent l'égalité et la justice, des actions plus cruciales à leurs yeux[15]. Par ailleurs, et cela n'a rien d'étonnant, les regroupements de hackeurs de gauche sont plus nombreux et plus actifs dans les sociétés qui possèdent des gauches socialistes et anarchistes bien établies — par exemple, l'Espagne, l'Italie, la Grèce, la Croatie ou l'Argentine (Bazzichelli, 2013 ; Corsin Jimenez et Estalella, 2016 ; Maxigas, 2012). Certains de ces constats s'expliquent très simplement. La mosaïque des sensibilités politiques des hackeurs correspond souvent à celle des populations dominantes dans les régions considérées — mais seulement jusqu'à un certain point. Les dimensions qui concernent plus particulièrement les tactiques des hackeurs et leur sociabilité politique s'avèrent plus singulières et propres au hacking lui-même.

14. « About us », Riseup.net, https://help.riseup.net/about-us.
15. Keizer (2012) propose un plaidoyer socialiste en faveur de la protection des données personnelles.

La plupart des hackeurs appuient sans réserve la diffusion transparente de l'information et le débat public. Nombreux sont toutefois les regroupements, notamment WikiLeaks et Anonymous, qui s'inscrivent en faux contre le fantasme libéral fondamental selon lequel les modalités conventionnelles du débat et les lieux officiels et légaux de l'action politique (en particulier, les partis et les élections) suffiraient pour catalyser le changement. Élaboration d'outils politiques, redéfinition du droit, fuitage d'information, diffusion d'alertes, et surtout, action directe : les tactiques des hackeurs témoignent d'un engagement politique immédiat et concret qui dépasse le simple attachement aux libertés civiles. Au-delà de la divulgation chère aux libéraux, ils entrent de plain-pied dans l'action, parfois même l'action directe illégale motivée par des principes pleinement assumés[16].

Les hackeurs se distinguent aussi par leur adhésion franche et massive à l'intersectionnalité politique, en ceci qu'ils n'éprouvent guère de difficultés à travailler entre « collègues » d'allégeances politiques divergentes. Le pragmatisme prenant généralement le pas sur l'idéologie, un anarchiste anticapitaliste peut très bien collaborer avec un social-démocrate libéral. Un cas bien connu illustrera ce constat. Le hackeur Jeremy Hammond, qui se revendique anarchiste, purge actuellement une peine de dix ans de prison pour des intrusions dans des systèmes informatiques et des actes de sabotage d'entreprise menés conjointement sous la bannière d'Anonymous. Depuis toujours, Hammond consacre l'essentiel de son temps à la destruction du capitalisme et de l'État libéral, et son but consiste à établir une société plus égalitaire par la mise en œuvre d'actions politiques anarchistes et écologistes souvent sans rapport avec la technologie. L'activisme d'Anonymous a néanmoins piqué sa curiosité de hackeur. Rebuté par les propos grossiers et souvent racistes que le collectif tolère dans ses rangs, Hammond a tout d'abord refusé de prendre part à ses projets. Puis, évaluant Anonymous à l'aune de ses exploits de hacking plutôt qu'à son style discursif, il a graduellement changé d'avis et a décidé finalement d'unir ses forces à celles du collectif pour une raison toute pragmatique : plus que l'absence de vision ou d'objectifs démocratiques clairement énoncés, c'est l'action qui compte[17].

16. Darin Barney (2013) défend de manière convaincante l'idée que WikiLeaks, généralement considéré comme une initiative typiquement libérale de publication des données, se démarque en réalité nettement de la logique libérale et privilégie au contraire des tactiques qui outrepassent le débat et menacent l'essence même de la gouvernance libérale. Johan Söderberg (2013) propose une argumentation très subtile, différente mais apparentée : les hackeurs sont farouchement attachés aux théories du déterminisme technologique, mais ils s'engagent quand même dans des actions collectives de lutte pour le changement. Söderberg souligne la discordance entre les théories déterministes et les pratiques politiques des hackeurs, mais il analyse aussi les mécanismes par lesquels les théories du déterminisme peuvent en définitive servir de bougie d'allumage à l'action.

17. Ainsi que me le faisait remarquer très justement un étudiant lors d'un atelier, le pragmatisme lui-même peut devenir une idéologie ; de fait, il peut être considéré comme une dimension politique essentielle chez le hackeur. Il reste néanmoins pertinent de souligner que cet attachement au pragmatisme, quelle que soit la définition qu'on en donne, permet à des hackeurs de travailler ensemble en dépit de leurs aspirations et buts politiques divergents.

Cela fait maintenant quinze ans que j'étudie les hackeurs, et j'ai maintes fois observé chez eux des raisonnements et des logiques similaires. L'inverse existe aussi : plusieurs collectifs technologiques de gauche dont il est question ici restent extrêmement méfiants et imposent des conditions très strictes d'adhésion à leurs aspirants membres. Par ailleurs, des subtilités linguistiques provoquent parfois de vraies querelles politiques internes : à la fin des années 1990, des membres du mouvement du logiciel libre/à code source ouvert en ont accusé d'autres de troquer le mot « libre » pour « ouvert » afin de séduire les investisseurs qu'un langage trop « chargé » politiquement risquait d'effaroucher (Berry, 2008).

Néanmoins, dans leurs regroupements de militantisme, piraterie, développement de logiciels ou autres activités, les hackeurs évitent généralement de se doter de lignes idéologiques communes — et se dispensent au passage d'avoir à en surveiller l'application (Postill, 2014, analyse le pragmatisme dans le hacking politique). Si, à l'instar du Projet Debian, la plupart de ces regroupements encadrent les modes de fonctionnement, les codes de conduite, voire les connaissances et compétences nécessaires, ils s'abstiennent généralement d'en faire autant pour les convictions politiques. Dans certains cas, cet « agnosticisme politique », pour reprendre un terme que j'ai proposé ailleurs (Coleman, 2013), découle d'une volonté de délimiter très précisément les buts du projet, souvent de manière strictement technique ou uniquement sous l'angle des libertés civiles. D'autres regroupements, par exemple Anonymous, adoptent une hybridité plus radicale : tenter de définir Anonymous au moyen de paramètres politiques exacts reviendrait à vouloir confiner son esprit et sa raison d'être dans une grille d'analyse trop rigide pour lui.

Il serait évidemment trop simpliste d'attribuer les traits caractéristiques de l'activisme politique des hackeurs (leur propension à ajouter l'action à la divulgation et leur inclination à coopérer entre eux malgré leurs différences idéologiques) uniquement aux savoir-faire intrinsèques du hacking et à sa nature fluide et ingénieuse — au fait que les hackeurs créent des dispositifs et résolvent des problèmes, mais toujours dans une optique d'acrobatie antiautoritaire. Il serait cependant tout aussi simpliste d'évincer ces deux traits de l'analyse.

CONCLUSION : L'ARSENAL DU GEEK

Engagements civiques libéraux visant l'amélioration du fonctionnement du gouvernement étatique ; projets anarchistes de développement de logiciels et de communautés en marge de l'économie capitaliste et des institutions politiques libérales… Ainsi que le montre cet article, les hackeurs s'investissent dans l'action politique de diverses manières et pour une multitude de motifs et d'objectifs. Indépendamment de cette hétérogénéité, plusieurs événements ont influé sur l'intensification récente de l'activisme politique des hackeurs — des « événements critiques », pour reprendre l'expression de l'historien Bill Sewell (2005). Ces tournants ont réorienté le hacktivisme de manière fondamentale en raison des changements qu'ils ont suscités sur le coup, mais aussi parce qu'ils servent maintenant de sources d'émulation. Si quelques-uns de ces

épisodes décisifs remontent aux premiers pas du hacking, les événements plus récents dont il a été question dans cet article les ont ensuite largement surpassés par l'onde de choc géopolitique qu'ils ont provoquée : tout d'abord, WikiLeaks, puis plusieurs années d'activité intense de la part d'Anonymous, et enfin, point d'orgue de cette série, la mégafuite orchestrée par Snowden.

Ces événements critiques s'inscrivent toutefois dans un contexte : en l'absence des conditions socioculturelles décrites dans cet article, sans doute ne se seraient-ils pas produits, du moins pas de manière aussi éclatante. Si l'activisme politique actuel des hackeurs s'exprime nécessairement de manières singulières et multiples, les traits caractéristiques analysés ici n'en dessinent pas moins un fonds commun de pratiques culturelles, de sensibilités, et même de tactiques politiques qui constituent en quelque sorte « l'arsenal du geek » — une modalité politique évidemment définie par opposition à ce que le politologue et anthropologue James Scott appelle « l'arsenal du faible » dans son livre sur la résistance politique paysanne « discrète » (1985). L'arsenal du faible se compose de tactiques qui sont mises en œuvre par des populations marginalisées du point de vue économique et qui ne semblent pas politiques à première vue — des petits gestes illicites, par exemple des comportements dilatoires qui ralentissent le travail ou du vandalisme. À l'inverse, l'arsenal du geek contient un large éventail d'interventions politiques en soi, reconnues comme telles, et déployées par des acteurs visibles et privilégiés évoluant au cœur même de la vie économique[18].

Pour qui connaît les travaux de Scott, il peut sembler bien ironique, voire complètement fallacieux, d'établir ainsi un parallèle entre les hackeurs et des gens qui comptent parmi les plus pauvres et les plus exploités de la société — des « subalternes ». Les travaux de Scott sur l'arsenal du faible nous intéressent néanmoins en ce qu'ils démontrent de façon magistrale que les manifestations politiques de la résistance comportent souvent une dimension logique et une dimension artistique, et qu'elles s'enracinent toutes deux dans des conditions matérielles et historiques. En tant que gens de métier, les hackeurs développent des habitudes de pensée critique indépendante, construisent des communautés et des infrastructures autonomes, et cherchent à réformer la loi ou à en nier la légitimité pour affirmer leur droit d'agir en tant que hackeurs. Inextricablement enchevêtrés à ce savoir-faire, l'astuce acrobatique et l'antiautoritarisme s'expriment à la mesure des tactiques d'action directe et des infractions qui caractérisent le hacktivisme actuel. Dans une certaine mesure, ils expliquent aussi pourquoi certains hackeurs se montrent si disposés à prendre de tels risques.

Pour que ces conditions et caractéristiques exercent une réelle influence sur les processus politiques, elles doivent toutefois être largement répandues, s'inscrire dans le parcours, non pas de quelques hackeurs isolés, mais d'un nombre important d'entre eux. Revenons à PW, ce hackeur hollandais établi à Toronto dont il était question au tout début de cet article. PW est convaincu du fait que les technologies et les événe-

18. Rosado-Murillo et Kelty (2017) proposent une analyse précise du positionnement de certaines tactiques politiques des hackeurs (par exemple, le fuitage d'information, l'intrusion dans des systèmes de sécurité, le piratage ou le déni de service) par rapport à diverses modalités du pouvoir.

ments peuvent jouer un rôle de premier plan dans la mobilisation politique. Son propre parcours présente d'ailleurs la plupart des caractéristiques et des traits socioculturels décrits dans cet article. Un rapide coup d'œil à sa page LinkedIn suffit à le démontrer : en marge de ses multiples expériences professionnelles, PW signale des engagements bénévoles et des appartenances à des espaces libres, des collectifs informels de hackeurs, des associations d'ingénierie, des organismes à but non lucratif de défense des libertés, et des instances de réflexion et d'action sur les politiques.

> Directeur de groupe de travail, rédacteur et membre de l'IETF (Internet Engineering Task Force)
> Member de la Electronic Frontier Foundation
> Cryptographe chez Cypherpunks
> Cofondateur de HackLab.TO
> Membre fondateur du Libreswan Project
> Membre du collectif Hippies from Hell [hackeur]

Comme PW, nombreux sont les hackeurs adeptes de l'arsenal du geek qui se fréquentent dans divers espaces publics ou projets collectifs. PW est ainsi membre de regroupements de ce type depuis plus de dix ans. D'autres pourraient s'investir dans des lieux différents. Par exemple, une hackeuse de gauche pourrait faire partie de plusieurs projets techniques, mais aussi de quelques incubateurs (*hack labs*) de gauche ou collectifs technologiques anarchistes. Les geeks et les hackeurs privilégient des orientations et même des configurations politiques très hétérogènes. Ils ne s'entendent pas non plus sur le meilleur moyen de faire advenir les changements sociaux. Néanmoins, ils présentent tous un point commun majeur : les outils politiques qu'ils créent et, dans une moindre mesure, leurs orientations tactiques (leur propension à travailler avec des collègues d'horizons politiques différents et, pour un nombre plus restreint d'entre eux, leur inclination à s'engager dans des actions directes illégales et risquées) émergent de leur pratique concrète du hacking, du « métier » de hackeur.

S'il se trouve actuellement en pleine floraison, l'activisme politique des hackeurs pourrait fort bien s'étioler demain si les circonstances lui devenaient moins propices. Parmi les nombreux écueils qui guettent la politisation des hackeurs, une culture commerciale très particulière la menace : l'entrepreneuriat de type Silicon Valley. Née en Californie, cette idéologie du développement des entreprises est aujourd'hui solidement implantée dans la plupart des grands centres urbains de la planète — New York, Austin, Denver, Boston, Shanghai, Londres, Berlin, etc. (voir Barbrook et Cameron, 1996 ; Marwick, 2013 ; Neff, 2012 ; Turner, 2006). Depuis très longtemps déjà, les forces économiques qui la sous-tendent phagocytent régulièrement les réflexions et projets autonomes des hackeurs, les mobilisent parfois dans de séduisants et médiatiques hackatons au service des impératifs commerciaux de l'entreprise (Irani, 2015), ou les cannibalisent de manière franche et directe en leur offrant une carrière ou un emploi qui promet de les propulser à titre individuel (Delfanti et Söderberg, 2015).

Comment cette dynamique va-t-elle évoluer ? Cela reste à voir. Un emploi régulier peut offrir la sécurité et le temps libre nécessaires pour s'investir dans des projets non commerciaux. Par ailleurs, une tradition bien ancrée chez les hackeurs de gauche consiste à subtiliser du temps de travail pour ériger ou entretenir des infrastructures autonomes de hacking — une opération de braconnage qui n'a somme toute rien d'une prouesse, les superviseurs dépourvus de formation technique s'avérant bien incapables de distinguer un écran vert d'un autre écran vert… Néanmoins, dans la mesure où les cultures technologiques de type Silicon Valley exigent un investissement considérable en temps et présentent le travail dans les industries technologiques capitalistes sous les atours d'une activité politiquement progressiste, leur expansion dans des régions de plus en plus étendues et nombreuses de la planète pourrait précipiter le déclin ou la perte du militantisme politique des hackeurs.

En dépit de cette menace, parmi bien d'autres, un constat majeur émerge de ces cinq dernières années : de nombreux hackeurs comprennent maintenant que leurs droits et ceux des autres resteront précaires tant qu'ils ne s'engageront pas très fermement dans une action politique qui dépasse leur propre univers et leurs préoccupations particulières. Naguère gens de métier autonomes et autocentrés, les hackeurs s'imposent aujourd'hui comme des activistes politiques pleinement assumés et mobilisés par des préoccupations qui ne les concernent plus toujours aussi directement. Cette transition nous montre que les événements ne suffisent pas ; les technologies ne suffisent pas ; le parti pris de la technologie ne suffit pas, ni les personnes en tant qu'individus, ni les espaces libres ou les communautés : rien de tout cela n'est fécond en soi. L'agglomération et la densification de tous ces éléments s'avèrent indispensables pour qu'ils portent leurs fruits. C'est l'ensemble de ces composantes qui procure les ressources et les infrastructures nécessaires pour susciter la volonté et la capacité d'agir dans la sphère politique — dans la mesure où les circonstances historiques s'y prêtent.

BIBLIOGRAPHIE

Barbrook, R. et A. Cameron (2009) [1996 pour la version originale anglaise], « L'idéologie californienne » (trad. de Pierre Blouin). Consulté à l'adresse https://charro1010.wordpress.com/2009/11/29/lideologie-californienne-par-richard-barbrook-et-andy-cameron-traduction-pierre-blouin/

Barney, D. (2013), « Publics without politics : surplus publicity as depoliticization », *in* Kozolanka K. et *al.* (dir.), *Publicity and the Canadian state : critical communications approaches,* Toronto, Presses de l'Université de Toronto, p. 72-88.

Bazzichelli, T. (2013), *Networked disruption : rethinking oppositions in art, hacktivism and the business of social networkin,* Aarhus, Aarhus Universitet Multimedieuddannelsen.

Berry, D. M. (2008), *Copy, rip, burn : the politics of copyleft and open source,* Londres, Pluto.

Beyer, J. L. (2014), *Expect us : online communities and political mobilization*, Oxford, Presses de l'Université d'Oxford.

Burkart, P. (2014), *Pirate politics : the new information policy contests*, Cambridge, MA, MIT Press.

Coleman, E. G. (2013), *Coding freedom : the ethics and aesthetics of hacking,* Princeton, NJ, Presses de l'Université de Princeton.

Coleman, E. G. (2016) [2014 pour la version originale anglaise], *Anonymous : Hacker, activiste, faussaire, mouchard, lanceur d'alerte*, (trad. de Nicolas Calvé), Montréal, Lux Éditeur.

Coleman, E. G. (2016), « Hackers », *in* Peters B. (dir.), *Digital keywords : a vocabulary of information society and culture*, Princeton, NJ, Presses de l'Université de Princeton, p. 158-172.

Collins, H. (2010), *Tacit and explicit knowledge*, Chicago, Presses de l'Université de Chicago.

Corsin, J. A. et A. Estalella (2016), « Ethnography : a prototype », *Ethnos*, vol. 82, n° 5, p. 846-866. doi : 10.1080/00141844.2015.1133688.

Delfanti, A. (2013), *Biohackers : the politics of open science*, Londres, Pluto.

Delfanti, A. et J. Soderberg (2015), « Hacking hacked ! the life cycles of digital innovation », *Science, Technology, and Human Values,* vol. 40, n° 5, p. 793-798.

Dreyfus, S. (2012) [1997 pour la version originale anglaise], « Underground », (trad. de Guillaume Boit), Paris, Éditions des Équateurs.

Golumbia, D. (2013), « Cyberlibertarians : digital deletion of the left », *Jacobin.* Consulté à l'adresse https://www.jacobinmag.com/2013/12/cyberlibertarians-digital-deletion-of-the-left/.

Goriunova, O. (dir.) (2014), *Fun and software : exploring pleasure, paradox and pain in computing*, New York, Bloomsbury Academic.

Greenberg, A. (2012), *This machine kills secrets : how WikiLeakers, cypherpunks, and hacktivists aim to free the world's information*, New York, Dutton Adult.

Irani, L. (2015), « Hackathons and the making of entrepreneurial citizenship », *Science, Technology, and Human Values,* vol.40, n° 5, p. 799-824.

Jordan, T. (2008), *Hacking : digital media and technological determinism*, Cambridge, Polity.

Jordan, T. et P. A. Taylor (2004), *Hacktivism and cyberwars : rebels with a cause ?,* London, Routledge.

Juris, J. S. (2008), *Networking futures : the movements against corporate globalization*, Durham, NC, Presses de l'Université de Duke.

Keizer, G. (2012), *Privacy*, New York, Picador.

Kelty, C. M. (2008), *Two bits : the cultural significance of free software*, Durham, NC, Presses de l'Université de Duke.

Kubitschko, S. (2015), « Hackers' media practices : demonstrating and articulating expertise as interlocking arrangements », *Convergence : The International Journal of Research into New Media Technologies,* vol. 21, n° 3, p. 388-402.

Lapsley, P. (2013), *Exploding the phone : the untold story of the teenagers and outlaws who hacked,* Ma Bell. New York, Grove.

Levy, S. (2001), *Crypto : how the code rebels beat the government, saving privacy in the digital age*, Londres, Penguin.

Levy, S. 2013 [1984 pour la version originale anglaise], *L'éthique des hackers*, (trad. de Gilles Tordjman), Paris, Éditions Globe.

Loveluck, B. (2015), « Internet, une société contre l'État ? », *Réseaux*, vol. 4, n° 192, p. 235-270.

Marwick, A. et D. Boyd (2011), « To see and be seen : celebrity practice on Twitter », *Convergence : The International Journal of Research into New Media Technologies,* vol. 17, n° 2, p. 139-158.

Maxigas, P. (2012), « Hacklabs and hackerspaces : tracing two genealogies », *Journal of Peer Production 2*. Consulté à l'adresse http://peerproduction.net/issues/issue-2/peer-reviewed-papers/hacklabs-and-hackerspaces/.

Mckelvey, F. (2014), « We like copies, just don't let the others fool you : the paradox of the Pirate Bay », *Television and New Media*, vol. 16, n° 8, p. 734-750.

The Mentor (1994), [1986 pour la version originale anglaise], « Le manifeste du hacker » (trad. de Neuralien) Source : NoWay3. Consulté à l'adresse http://elskate4.chez-alice.fr/Labbai-and-Ari/manifeste.htm

Milan, S. (2013), *Social movements and their technologies*, London, Palgrave.

Milberry, K. « (Re)making the Internet : free software and the social factory hack », in M. Ratto et M. Boler (dir.), *DIY citizenship : critical making and social media*, Cambridge, MA, MIT Press.

Mills, E. (2008), « Social engineering 101 : Mitnick and other hackers show how it's done ». *CNET*. Consulté à l'adresse http://www.cnet.com/news/social-engineering-101-mitnick-and-other-hackers-show-how-its-done/.

Montfort, N. (2008). « Obfuscated code », in M. Fuller (dir.), *Software studies : a lexicon,* Cambridge, MA, MIT Press, p. 193-199.

Neff, G. (2012), *Venture labor : work and the burden of risk in innovative industries*, Cambridge, MA, MIT Press.

O'neil, M. (2009), *Cyberchiefs : autonomy and authority in online tribes,* London, Pluto.

Orr, J. E. (1996), *Talking about machines : an ethnography of a modern job*, Ithaca, New York, ILR Press.

Peterson, T. F. (2011), *Nightwork : a history of hacks and pranks at MIT*, Cambridge, MA, MIT Press.

Polanyi, M. (1967), *The tacit dimension*, New York, Anchor.

Polletta, F. (1999), « 'Free spaces' in collective action », *Theory and Society* vol. 28, n° 1, p. 1-38.

Postigo, H. (2012), *The digital rights movement : the role of technology in subverting digital copyright,* Cambridge, MA, MIT Press.

Postill, J. (2014), « Freedom technologists and the new protest movements : a theory of protest formulas », *Convergence : The International Journal of Research into New Media Technologies,* vol. 20, n° 4, p. 402-418.

Rosado-Murillo, L. F. et C. M. Kelty (2017), « Hacking und hackers », *in* Koch G. (dir.), *Digitalisierung : Theorien und Konzepte für die Empirische Forschung*, Konstanz, Presses d'UVK. À paraître.

Sauter, M. (2014), *The coming swarm : DDOS actions, hacktivism, and civil disobedience on the Internet*, New York, Bloomsbury Academic.

Schoen, S. (2001), « How to decrypt a DVD : in haiku form. (Thanks, Prof. D. S. T.) » Consulté à l'adresse https://www.cs.cmu.edu/~dst/DeCSS/Gallery/decss-haiku.txt.

Schrock, A.R. (2016), « Civic hacking as data activism and advocacy : a history from publicity to open government data », *New Media and Society,* vol. 18, n° 4, p. 581-599.

Scott, J. (1985), *Weapons of the weak : everyday forms of peasant resistance*, New Haven, CT, Presses de l'Université de Yale.

Sennett, R. (2010) [2009 pour la version originale anglaise], *Ce que sait la main : La culture de l'artisanat* (trad. de Pierre-Emmanuel Dauzat), Paris, Albin Michel.

Sewell, W. H. (2005), *Logics of history : social theory and social transformation*, Chicago, Presses de l'Université de Chicago.

Soderberg, J. (2007), *Hacking capitalism : the free and open source software movement*, London, Routledge.

Soderberg, J. (2013), « Determining social change : the role of technological determinism in the collective action framing of hackers », *New Media and Society,* vol.15, n° 8, p. 1277-1293.

Sterling, B. (1992), *The hacker crackdown : law and disorder on the electronic frontier*, New York, Bantam.

Straw, W. (2014), « Some things a scene might be », *Cultural Studies*, vol. 29, n° 3, p. 476-485.

Thomas, D. (2003), *Hacker culture*, Minneapolis : Presses de l'Université de Minnesota.

Thompson, E. P. (2015) [1978 pour la version originale anglaise intitulée *Poverty of Theory*], *Misère de la théorie,* (trad. de Alexia Blin, Antony Burlaud, Yohann Douet et Alexandre Feron), Paris, Éditions L'échappée.

Thorsen, E., C. Sreedharan et S. Allan (2013), « WikiLeaks and whistle-blowing : the framing of Bradley Manning », *in* Brevini B., A. Hintz et P. Mccurdy (dir.), *Beyond WikiLeaks : implications for the future of communications, journalism and society*, New York, Palgrave Macmillan, p. 101-122.

Turner, F. (2013) [2006 pour la version originale anglaise], *Aux sources de l'utopie numérique. De la contre culture à la cyberculture : Stewart Brand, un homme d'influence* (trad. de Laurent Vannini), C&F Éditions.

Wark, M. (2006) [2004 pour la version originale anglaise], *Un Manifeste Hacker* (trad. de Club Post-1984 Mary Shelley & Cie Hacker Band), Éditions Criticalsecret, Paris.

Warner, M. (2002), *Publics and counterpublics*, New York, Zone.

Wolfson, T. (2014), *Digital rebellion : the birth of the cyberleft,* Urbana- Champagne, Presses de l'Université d'Illinois.