“ Il faut défendre la société de contrôle ”: Les hackers face au libéralisme autoritaire

Félix Tréguer

« Il faut défendre la société de contrôle » : Les hackers face au libéralisme autoritaire*

Félix Tréguer**

Juin 2021

Résumé

Après avoir rappelé la filiation entre les pionniers du militantisme hacker et les tactiques anti-technocratiques engagées par la Nouvelle Gauche, cet article propose d'interpréter la vague répressive qui frappa les hackers à la fin des années 1980 comme l'une des stratégies de pouvoir conçues pour refermer la crise de gouvernementalité engagée dans les années 1960 – une stratégie depuis réactivée chaque fois qu'un « front hacker » a semblé sur le point de se reconstituer. Ce faisant, il invite à voir dans cet épisode de sécurisation du cyberespace et de répression des répertoires d'action transgressifs un moment critique dans la généalogie du libéralisme autoritaire.

After recalling the lineage between hacktivist pioneers and the anti-technocratic tactics of the New Left, this article construes the repressive wave that hit hackers at the end of the 1980s as one of the power strategies designed to close the crisis of governmentality initiated in the 1960s – a strategy that has since been reactivated whenever a "hacker front" seemed about to materialise. In so doing, it analyses this securitisation of cyberspace and the repression of transgressive action repertoires it entailed as a critical moment in the genealogy of authoritarian liberalism.

*Article paru dans la revue Quaderni n°103, *Politiques du hacking*, numéro dirigé par Benjamin Loveluck et Jean-Vincent Holeindre (printemps 2021).

**Félix Tréguer est post-doctorant au CERI Sciences Po et chercheur associé au Centre Internet et Société du CNRS. Il est membre fondateur de La Quadrature du Net, une association dédiée à la défense des libertés dans le contexte d'informatisation, et l'auteur de *L'utopie déchue : une contre-histoire d'Internet, XV^è-XXI^è siècle* (Fayard, 2019).

Introduction : l'hacktivisme hors-jeu ?

Au tournant des années 1980, Gilles Deleuze tente de cerner les « sociétés de contrôle » caractéristiques de la modernité tardive. Prolongeant les analyses de Michel Foucault sur le pouvoir, il remarque qu'à la différence des châtiments exemplaires hérités de l'ère féodale et des logiques disciplinaires typiques des régimes libéraux, les formes les plus actuelles du contrôle social opèrent « non plus par enfermement, mais par contrôle continu et communication instantanée », sur des modes « toujours plus immanents au champ social, diffusés dans le cerveau et le corps de citoyens » (Deleuze 1990). L'ordinateur et les réseaux informatiques constituent la clé de voûte de ce nouveau régime de pouvoir : « Ce qui compte, écrit-il, ce n'est pas la barrière, mais l'ordinateur qui repère la position de chacun, licite ou illicite, et opère une modulation universelle ».

Si le philosophe reconnaît que l'informatique et les dispositifs sécuritaires qu'elle sous-tend sont particulièrement insidieux, il estime cependant qu'« il n'y a pas lieu de demander quel est le régime le plus dur, ou le plus tolérable, car c'est en chacun d'eux que s'affrontent les libérations et les asservissements ». Ce qu'il faut, c'est « chercher de nouvelles armes ». Or, pour Deleuze, la complexité croissante des machines constitue autant de points de faiblesse :

> Les vieilles sociétés de souveraineté maniaient des machines simples, leviers, poulies, horloges ; mais les sociétés disciplinaires récentes avaient pour équipement des machines énergétiques, avec le danger passif de l'entropie, et le danger actif du sabotage ; les sociétés de contrôle opèrent par machines de troisième espèce, machines informatiques et ordinateurs dont le danger passif est le brouillage, et l'actif, le piratage et l'introduction de virus.

Lorsque Deleuze écrit ces lignes, le personnage du « pirate informatique » s'est imposé dans les imaginaires. Depuis quelques années, les transgressions et autres illégalismes[1] hackers font les gros titres, au point qu'ils apparaissent pour de nombreux observateurs d'alors comme la figure archétypale de la désobéissance aux sociétés de contrôle. Le poète anarchiste Hakim Bey, dans son célèbre essai paru en 1991 sur les « zones d'autonomie temporaire », loue à son tour la « guérilla du *hacking* ». Il y voit la marque à la fois du « chaos » qui tourmente l'infrastructure numérique et la possibilité « de tirer avantage des perturbations, des ruptures ou des crashs du Net » (Bey 2003).

Les hackers constituent dès l'origine une nébuleuse particulièrement diverse, tant en termes de pratiques que d'idéologies – sans doute faudrait-

[1] Le terme « illégalisme » est utilisé par Michel Foucault pour désigner « l'ensemble des pratiques qui soit transgressent délibérément, soit contournent ou même détournent la loi » (Gros 2010).

il d'ailleurs davantage parler du *hacking* comme pratique que des *hackers* entendus comme un groupe social homogène. Au sein de cette mouvance – parfois au sein d'un même collectif –, on trouve en effet une diversité de positionnements politiques, que ce soit vis-à-vis de l'État, du capitalisme ou de la technologie. Pourtant, en ce début des années 1990, sa minorité militante captive les imaginaires et nourrit les espoirs politiques d'une partie de la gauche radicale. C'est qu'avec elle, l'action directe[2] se déployait là où on l'attendait le moins, à savoir au sein-même des infrastructures numériques des grandes organisations bureaucratiques.

En pénétrant illégalement dans leurs systèmes informatiques pour révéler des failles de sécurité ou faire fuiter des informations secrètes, en pratiquant le sabotage, en développant des applications civiles de cryptographie pour désarmer la surveillance d'État, les hackers n'entendaient plus seulement œuvrer, dans une veine « expressiviste »[3], à la construction d'une informatique alternative et émancipatrice (par exemple en mettant en place des serveurs autogérés contribuant à l'autonomie médiatique des mouvements sociaux) (Cardon et Granjon 2010). Désormais, ils se livraient également à des tactiques « anti-hégémoniques » destinées à entraver les machines du pouvoir.

Trente ans plus tard, les espoirs soulevés par l'émergence de l'« hacktivisme » – un néologisme qui renvoie au croisement entre les ruses hackers et l'action directe (Jordan et Taylor 2004) – semblent avoir été déçus. Dans les régimes représentatifs d'Europe ou d'Amérique du Nord, malgré quelques coups d'éclats spectaculaires, la mouvance hacktiviste est aujourd'hui sur la défensive. L'année 2013 paraît avoir constitué de ce point de vue un tournant. À l'époque, Julian Assange, le fondateur de WikiLeaks, s'adressait encore aux « administrateurs systèmes » lors d'un congrès de hackers en Allemagne en les appelant à développer une conscience de classe. Tentant un parallèle avec les ouvriers prolétaires du XIX^{è} siècle, et dans un clin

[2]L'action directe, théorisée au sein de la mouvance anarcho-syndicaliste au début du XX^{è} siècle, correspond à des formes d'engagement politiques qui voient les militants s'organiser pour atteindre leurs objectifs par leurs propres moyens, quitte à enfreindre la loi, plutôt que d'en appeler aux institutions représentatives et d'inscrire leur action au sein des cadres juridiques, politiques et économiques dominants. L'action directe non-violente recouvre des modes d'action tels que les sit-ins, les grèves, les occupations, ou la création de systèmes de production et d'échange alternatifs. L'action directe violente renvoie à des actes politiques recourant à la violence physique ou symbolique (cette dernière recouvrant notamment les destructions matérielles ou le sabotage).

[3]La distinction opérée ici entre critique « contre-hégémonique » et critique « expressiviste » s'inspire des travaux de Cardon et Granjon (2010) sur le « médiactivisme ». Elle peut par analogie s'appliquer au champ de l'hacktivisme et de l'activisme numérique en général : la critique anti-hégémonique de l'informatique porte ainsi en priorité sur la dénonciation du modèle dominant d'informatisation, vecteur des pouvoirs économiques et politiques ; la critique expressiviste se consacre pour sa part à la construction d'une informatique alternative capable de soutenir les capacités émancipatrices et les potentialités d'expression des sujets.

d'œil à Marx et Engels, il lançait l'appel « *Sysadmins of the world, unite !* » (Borland 2013). Tout cela paraît désormais bien lointain. Alors que les crises successives démultiplient les dispositifs numériques de contrôle social, l'opposition à l'informatique dominante n'a évidemment pas disparu – qu'on pense par exemple aux mobilisations récentes contre les algorithmes de classement des bacheliers, contre les nouvelles technologies de surveillance policières, ou même contre la 5G. Mais bien souvent, ces oppositions demeurent cantonnées à des protestations isolées ou à des stratégies légalistes devant les parlements ou les tribunaux – autant de modes d'action conventionnels dont l'efficacité paraît en pratique bien limitée.

L'hacktivisme perdure certes sous ses formes expressivistes, par exemple à travers la maintenance de réseaux télécoms ou de serveurs auto-gérés. Ces alternatives paraissent cependant condamnées à une certaine marginalité à l'heure où les géants de l'économie numérique renforcent leurs positions dominantes, aspirant une part toujours plus conséquente du « web militant » et exposant ses participants aux nouveaux assemblages public-privé dédiés à la surveillance et à la censure. Quant aux initiatives visant à dénoncer et à entraver l'informatique hégémonique à travers des formes plus confrontationnelles d'action directe, elles sont aujourd'hui réduites à portion congrue. Si des destructions physiques d'antennes-relais ou de câbles de fibre optique émaillent parfois l'actualité, la frange hacktiviste, quant à elle, semble pratiquement hors-jeu. Après avoir vu certaines de ses plus éminentes figures subir l'exil ou l'emprisonnement, elle paraît en fait abasourdie par la violence de sa confrontation avec le pouvoir.

Comment expliquer ce qui apparaît comme un affaiblissement historique de l'hacktivisme ? Plusieurs facteurs méritent d'être étudiés pour expliquer cette évolution. Dans cet article, j'aimerais me concentrer sur l'un de ceux qui me paraît le plus significatif, à savoir la violente répression essuyée par la mouvance au tournant des années 1980, en proposant de la réinscrire dans une séquence historique plus longue. Car au-delà du fait qu'elle constitue l'épisode inaugural du traitement d'exception généralement réservé à l'action politique sur Internet, on peut aussi l'interpréter comme la fin de quelque chose : en venant disqualifier, sur les plans juridique et politique, certains modes d'action directe prenant pour cible les infrastructures informatiques dominantes, cette vague répressive venait refermer le cycle de contestation anti-technocratique ouvert dans les années 1960. Après des années d'opposition à l'informatisation, elle traduisait ce nouvel impératif du pouvoir : défendre la société de contrôle[4].

[4]L'expression « défendre la société de contrôle », également présente dans le titre de cet article, fait allusion au cours donné par Michel Foucault au Collège de France en 1976 « Il faut défendre la société » (Foucault 1997).

1. Les hackers militants, continuateurs des luttes anti-technocratiques des années 1960

Au début des années 1980, l'informatique accompagne la financiarisation du capitalisme international et pénètre désormais dans les foyers des classes aisées. L'ordinateur – devenu personnel – semble alors emporter l'adhésion du public. Après les contestations des années 1960 et 1970 contre le « technocratisme » – cet amalgame des sciences et de la rationalité bureaucratique conduisant, comme le résume le philosophe Andrew Feenberg, à un « système administratif tentaculaire qui se réclame, pour se légitimer, de l'expertise scientifique plutôt que de la tradition, du droit ou de la volonté des individus » (Feenberg 2004) –, la période est marquée par le retour en force d'un certain consensus autour du système dominant. C'est dans ce contexte qu'une avant-garde fait son apparition : les hackers.

Tantôt célébrés et tantôt conspués pour leurs ruses teintées de prudence et leur style parfois empreint d'orgueil, la minorité militante de la mouvance hacker proposa toute une série d'interventions destinées à perturber et à saboter les infrastructures informatiques déployées par les grandes organisations, qui s'informatisaient alors massivement. Chez les hackers des années 1980, il n'y a pas seulement une volonté de « retourner » l'informatique pour la faire fonctionner à des fins plus « démocratiques » – une dimension « expressiviste » sur laquelle insiste l'essentiel de l'historiographie (cf. Turner 2012). Il y a aussi la reprise de logiques d'action directe visant les infrastructures informatiques des grandes bureaucraties. Or, ces modes d'action spontanément analysés comme des innovations militantes peuvent en réalité s'interpréter comme la transposition dans l'espace numérique de certaines tactiques anti-technocratiques développées par des groupes militants issus de la « Nouvelle Gauche »[5] à partir des années 1960.

Certains travaux ont déjà eu l'occasion de mettre l'accent sur cette filiation anti-hégémonique, à l'image de l'anthropologue Gabriella Coleman. Dans ses recherches sur la généalogie hacker, Coleman (2012) fait ainsi le lien entre un groupe emblématique de la Nouvelle Gauche étasunienne – les Yippies – et la pratique hacker du *phreaking* – un terme issu de la contraction des mots « *phone* » et « *freak* » qui désigne les pratiques techniques permettant l'utilisation gratuite et le détournement des réseaux télécoms à des fins souvent potaches ou pour dénoncer des failles de sécurité. Mais cette continuité avec la Nouvelle Gauche semble valoir pour bien d'autres modes d'action hackers.

À partir des années 1960, en Europe et aux États-Unis, les mouvements

[5]Le terme de « Nouvelle Gauche » renvoie aux différents mouvements d'inspiration marxiste et libertaire qui se déploient dans les années 1960 et 1970 en marge du mouvement ouvrier traditionnel et qui contribuent à « politiser » des aspects de l'existence considérés jusque-là comme extérieurs au champ politique.

associés à la Nouvelle Gauche ont en effet multiplié les innovations tactiques pour tenter d'ébranler l'informatique dominante. À l'époque, les groupes qui la composent s'éloignent du marxisme orthodoxe et de ses formes militantes incarnées par le Parti communiste pour tenter de refonder l'analyse de la société d'après-Guerre et développer des modalités de contestation adaptées à cette nouvelle donne socio-politique. Le processus de modernisation et la science elle-même sont pointés du doigt pour leur inféodation aux impératifs industriels et militaires, ainsi que pour leur rôle dans l'avènement de formes de vie totalitaire. Et s'il y a une technologie qui, à l'époque, incarne mieux que toute autre cette technocratie tant redoutée, c'est bien l'ordinateur.

En 1962 aux États-Unis, l'organisation phare de la Nouvelle Gauche, la Students for a Democratic Society (SDS) publie son « agenda pour une génération », sorte de programme militant qui affirme son « opposition totale à la coagulation bureaucratique et aux définitions des besoins humains en fonction des problèmes les plus aisément traitables par les ordinateurs ». Les nouvelles technologies comme l'informatique ou le nucléaire apparaissent essentiellement anti-démocratiques puisqu'elles nécessitent tout à la fois « expertise militaire, compréhension scientifique, et le manteau du secret » (SDS 1962).

En France, deux textes parus en 1967 et associés au mouvement situationniste s'inscrivent dans cette même veine anti-technocratique : *Traité de savoir-vivre à l'usage des jeunes générations* de Raoul Vaneigem, et *Contre les technocrates* d'Henri Lefebvre. Poursuivant tout en les critiquant les analyses des philosophes de l'École de Francfort ou de penseurs critiques de la technologie comme Jacques Ellul, l'un et l'autre nourrissent la critique d'une modernisation assimilée à un processus de déshumanisation. Vaneigem raille ainsi la manière dont « l'organisation sociale hiérarchisée construit le monde en détruisant les hommes » : « le perfectionnement de son mécanisme et de ses réseaux la fait fonctionner comme un ordinateur géant dont les programmateurs sont aussi programmés », tandis que « le plus froid des monstres froids trouve son accomplissement dans le projet d'État cybernétisé » (Vaneigem 1967). Henri Lefebvre souligne pour sa part que le pouvoir adjoint désormais à la « planification » et à la « consommation dirigée » la « quantification généralisée » et la « mise en carte perforée des masses humaines » (Lefebvre 1967). Dans ce contexte, l'action politique doit renouer avec la créativité : « À l'ère du calcul et à l'ère du soupçon inaugurées par le capitalisme et le stalinisme », écrit Vaneigem, « s'oppose et se construit dans une phase clandestine de tactique l'ère du jeu ».

Pour critiquer l'hégémonie technocratique et ses machines, les jeunes militants des années 1960 pratiquent donc le détournement, à l'image de ces étudiants de Berkeley engagés dans le Free Speech Movement qui, en décembre 1964, manifestent en s'attachant autour du cou les cartes perforées des ordinateurs de l'université. À la fin de la décennie, les activistes du SDS

s'adonnent également à des « occupations » sur les campus pour protester contre les projets de recherche associés au complexe militaro-industriel, dont certains mêlent déjà informaticiens et spécialistes des sciences comportementales (Levine 2018).

Bientôt, les franges les plus radicales de la Nouvelle Gauche se livrent même à des opérations de sabotage contre des installations informatiques associées au complexe militaro-industriel. Plusieurs actes de destruction matérielle visant les équipements informatiques d'universités sont notamment recensés à travers les États-Unis. En 1969, dans le Michigan, cinq membres d'un groupe opposé à la guerre du Vietnam et se faisant appeler les « Beaver 55 » s'en prennent aux ordinateurs d'une entreprises de chimie (Campbell 1992). Leur objectif consiste à détruire les données informatiques relatives à des programmes de recherche en lien avec les guerres menées par les États-Unis.

En Europe, à partir de la seconde moitié des années 1970, divers groupes d'extrême gauche s'adonnent à des actes semblables. Les Brigades Rouges italiennes ciblent ainsi plusieurs centres informatiques à partir de 1976. Dans leurs « vingt thèses finales », elles s'en justifient en décrivant l'ordinateur comme un engin militaire, « instrument du système capitaliste » et de la « guerre des classes », « la base matérielle "technique" de l'information et du contrôle total » (Brigades Rouges 1980). En France, entre 1980 et 1983, le « Comité liquidant ou détournant les ordinateurs », ou CLODO, défraie la chronique au gré d'une série d'actions incendiaires prenant pour cible des installations informatiques dans la région de Toulouse, haut lieu de l'industrie informatique nationale. Dans les textes revendiquant ces destructions matérielles qui circulent alors dans la presse, les membres non-identifiés du CLODO se présentent comme des « travailleurs de l'informatique » et décrivent l'ordinateur comme « le serviteur zélé du système dans lequel nous vivons », un dispositif « sans doute perverti par ses origines mêmes », et notamment « l'abus du quantitatif ou la réduction au binaire ». « Dans notre monde » affirment les auteurs, il n'est qu'« un outil de plus, particulièrement performant, au service des dominants (...) » (Izoard 2010).

Au total, une source évoque plus de deux cents cas de sabotage recensés sur une vingtaine d'années (Bequai 1987). Ces actes de destruction matérielle font tâche d'huile : lors des conflits sociaux suscités par l'informatisation croissante du secteur tertiaire à la fin des années 1970, des salariés n'hésitent plus à s'échanger des techniques rudimentaires dédiées au sabotage d'ordinateurs (Izoard 2010). Puis, quelques années plus tard, des collectifs hackers envisagent de les reprendre à leur compte, cherchant à enrayer les systèmes informatiques des États ou des grandes entreprises à travers l'introduction à distance de bugs, de virus ou l'effacement des données. Pour Gareth Branwyn, un journaliste qui prend part à plusieurs de ces groupes à la fin des années 1980, « les possibilités pour une insurrection et une égalité

des armes qui ne soit pas fondée sur la force brute changeait radicalement avec l'avènement des réseaux informatiques, et la dépendance presque totale de notre société à leur égard » (Lunceford 2009).

Outre les actes de sabotage matériel, des collectifs ou individus associés à la Nouvelle Gauche innovent aussi en multipliant les fuites d'informations secrètes. Au début des années 1970, c'est grâce à des lanceurs d'alerte et à des « vols » de documents que les programmes de surveillance des services de police et de renseignement – alors en cours d'informatisation – font scandale. Quelques années plus tard, les hackers tenteront à leur tour de systématiser les fuites de données pour tenir en échec le secret d'État et le secret des affaires. Toujours dans les années 1970, pour protéger la vie privée et la confidentialité des communications, de jeunes mathématiciens travaillent à extirper la cryptographie de son giron militaire (Corrigan-Gibbs 2014). Leurs avancées conceptuelles conduisent dix ans plus tard aux percées des « cypherpunks », ce groupe hacker qui au tournant des années 1980 œuvra à démocratiser la cryptographie, non seulement pour tenter d'immuniser la population des systèmes de surveillance d'État mais aussi protéger les lanceurs d'alerte et ainsi multiplier les fuites d'actifs informationnels (l'organisation WikiLeaks, lancée en 2006, incarne la concrétisation la plus retentissante de ces vieux projets) (Beltramini 2020).

Au regard de ces précédents, les formes d'action directe pratiquées par les hackers des années 1980 pour entraver le modèle hégémonique d'informatisation n'apparaissent pas tant comme des innovations fondatrices d'un « nouvel art de la révolte » que la transposition, sur les réseaux informatiques, des modes de résistance aux sociétés de contrôle qui s'étaient déployés avec vigueur depuis les années 1960 à travers la focale anti-technocratique. À l'image des tactiques de la résistance ordinaire étudiées par Michel de Certeau, les modes d'action hacktivistes peuvent ainsi s'analyser comme des composites réalisés à partir de « vocabulaires de langues reçues » et de « syntaxes prescrites » (Certeau 1990), dont certaines étaient directement héritées de la Nouvelle Gauche.

Or, à la fin des années 1980, au moment-même où les hackers étaient célébrés comme nouvelle avant-garde militante, ils firent l'objet d'une violente répression. Esquissant le prototype d'une « police du cyberespace », cet épisode semble également pouvoir s'interpréter comme l'un des fronts d'une stratégie de *containment* destinée à refermer la phase de contestation anti-technocratique ouverte dans les années 1960.

2. Répression et disqualification des illégalismes hackers

Pour faire sens de cette vague répressive, il est utile de revenir à la notion de « crise de gouvernementalité » dégagée par Michel Foucault. À travers elle, Foucault désigne les contradictions internes du libéralisme dans son articulation à la raison d'État ; ces moments où le pouvoir prend conscience du coût économique et politique que représente le « libre exercice » des libertés, lorsque le « trop-plein » de revendications devient générateur d'ingouvernabilité (Foucault 1994, 70). Dans son cours du 24 janvier 1979, Foucault donne l'exemple de la Commission Trilatérale. En 1975, ce club élitaire a publié *Crisis of Democracy*, un rapport rédigé par un groupe d'intellectuels comprenant notamment Samuel Huntington ou le sociologue français Michel Crozier (Crozier et al. 1975). Leur objectif est d'identifier des solutions à la crise de gouvernementalité induite par les contestations tous azimuts qui se font jour à l'époque, laquelle traduit selon eux des « excès de la démocratie » et montre l'urgente nécessité de « restaurer le prestige et l'autorité des institutions du gouvernement central. »

Plus récemment, le philosophe Grégoire Chamayou (2018) s'est également intéressé à cette crise de gouvernementalité associée aux années 1960-1970 à partir du dispositif spécifique de l'usine. Rappelant l'ampleur des « indisciplines ouvrières » (sabotage sur le chaînes de montage, absentéisme, etc.), Chamayou montre comment s'est construit en réaction une « révolution managériale » qui fait date dans l'histoire du « libéralisme autoritaire » – un concept forgé en 1933 par le juriste allemand antifasciste Hermann Heller pour qualifier un régime politique où l'État garantit la liberté des marchés tout en s'abritant des revendications démocratiques et sociales au moyen de la répression et du musellement des libertés publiques (Chamayou et al. 2020).

Or, la répression des hackers qui s'enclenche dans les années 1980 peut elle aussi s'analyser comme une réaction des autorités face à cette grande crise de gouvernementalité engagée dans les années 1960. Confrontés à la prolifération des tactiques militantes anti-technocratiques au sein de groupes associés à la Nouvelle Gauche, puis menacés par leur transposition dans l'environnement numérique par des informaticiens militants, les États et les grandes entreprises se devaient de protéger cette infrastructure technologique devenue vitale. D'où diabolisation des hackers et la guerre menée « pour l'exemple » à la mouvance hacktiviste.

L'urgence à agir est d'autant plus grande que, à l'heure où l'ordinateur sort enfin des grandes bureaucraties, les illégalismes politiques des hackers se banalisent au point de les rendre socialement acceptables dans un milieu informaticien alors en proie à une taylorisation croissante des tâches, notamment dans le secteur de la programmation (Kraft 1977). De fait, l'essentiel

des actes de sabotage ou d'intrusion informatique constatés par les autorités émanent de salariés (Ross 1990, Duff et Gardiner 1996). Il s'agit généralement d'anciens employés qui souhaitent ainsi se venger de leur hiérarchie ou qui ont pu faire le choix d'amener la résistance à l'informatisation à l'intérieur de leurs entreprises. En 1991, tout en estimant que le « pragmatisme » imposerait « de faire de l'informatique un domaine de haute sécurité », des chercheurs soulignent que, face à cette « nouvelle délinquance », « le groupe social des praticiens de l'informatique n'oppose qu'une très faible résistance » :

> Non seulement cette délinquance n'apparaît pas violente mais elle apparaît paradoxalement comme une contre-réaction légitime à la violence des ordinateurs et à l'emprise des réseaux techniques. Même l'argent détourné peut être considéré dans cette optique comme le juste salaire d'une compétence spécifique : dénoncer la toute-puissance des ordinateurs, sorte de revanche contre les menaces des "intelligences artificielles" (Breton et al. 1991).

À longueur de rapport, les autorités insistent sur la nécessité de résorber ce qui menace de se transformer en « zone de non-droit », mais aussi le formidable coût de ce nouveau type de délinquance en « col blanc ». Dans une étude du Sénat français dédié à la fraude informatique et publié en octobre 1987, les parlementaires relaient des « estimations américaines » qui font état de pertes de 100 millions de dollars à l'échelle fédérale. Tout en regrettant qu'« aucune statistique vraiment pertinente n'ait pu être établie », les auteurs du rapport reprennent néanmoins les conclusions du secteur des assurances selon lesquelles « les fraudes, sabotages ou indiscrétions (...) constitu[ent] pour l'avenir le risque potentiel le plus menaçant et le plus coûteux » (Thyraud 1987).

Outre le fait que leurs illégalismes en viennent à menacer le vaste mouvement d'informatisation de l'économie, les hackers sont aussi perçus comme une menace directe pour la souveraineté des États. Insaisissables, organisés en réseau à l'échelle transnationale, les « pirates informatiques » des années 1980 font écho, dans l'imaginaire policier, aux « pirates de l'air » islamistes des années 1970 et aux groupes terroristes d'extrême-gauche. En cette fin de guerre froide, au sein des agences de renseignement et dans les cercles militaires, ils sont aussi parfois présentés comme une nouvelle incarnation d'un terrorisme international piloté depuis l'URSS. Alors, face à leur supériorité technique et au « mauvais exemple » qu'ils offrent à toute une profession, les élites s'entendent pour engager un processus de sécurisation[6].

[6]La notion de « sécurisation » renvoie à ces actes de parole et autres discours d'autorité venant qualifier un objet donné de menace existentielle pour la société, afin « d'en appeler

L'enjeu consiste à pacifier l'informatique en réseau, le tout à grand renfort d'une rhétorique médicale évoquant la propagation « épidémique » de leurs illégalismes et la prolifération des « virus informatiques », et ce à l'heure où l'autre menace émergente est celle du sida.

Au cours des années 1980, sous l'impulsion des États-Unis relayée par des organisations internationales comme l'OCDE, les autorités nationales se dotent bientôt d'un cadre juridique visant à réprimer la « fraude informatique ». Bien souvent, à l'image de la France ou des États-Unis, la compétence pour prévenir et réprimer ce nouveau type de délinquance « hi-tech » est confiée aux services secrets, comme pour mieux marquer la gravité de cette menace. D'ailleurs, ces agences déploient rapidement leurs pratiques d'exception contre la mouvance hacktiviste : surveillance extra-légale des communications, infiltration, chantage et menaces en tous genres (Guisnel 1995). Quant aux peines encourues, elles se veulent dissuasives : aux États-Unis, le Computer Fraud and Abuse Act de 1986 prévoit une peine allant jusqu'à 20 ans de prison pour l'accès non-autorisé à des systèmes informatiques.

Une fois les législations pénales en place, plusieurs grandes vagues répressives frappent la mouvance (Sterling 1993). Chez les groupes hackers engagés dans une démarche politique, il y a le sentiment d'être injustement pris pour cible. En Allemagne ou en France, le plus vieux groupe hacktiviste d'Europe, le Chaos Computer Club (CCC) allemand, est évoqué lors des travaux parlementaires autour des lois destinées à réprimer le « piratage informatique » et fait office de bouc émissaire. Au printemps 1988, l'un des porte-paroles du CCC est même accusé (à tort) par les autorités françaises d'espionnage économique visant des organismes publics et privés associés à la recherche spatiale et militaire. Détenu pendant soixante-six jours à la prison de Fresnes, il est finalement relâché mais l'épisode illustre bien les effets de l'engrenage répressif sur ceux qui, quelques années plus tôt, pouvaient encore se présenter comme d'honorables défenseurs de la vie privée, avec la bienveillance des médias.

Au milieu années 1990, l'objectif semble atteint : les hackers dans leur ensemble apparaissent désormais comme déviants et leur frange hacktiviste est durablement stigmatisée (Nissenbaum 2005), au point que les années 1980 resteront dans les mémoires comme l'« âge d'or » du hacking (Thomas 2005). Quant à l'essentiel de la profession informaticienne, l'évolution du marché du travail contribue à assurer sa loyauté, les programmeurs et autres administrateurs système voyant leur capital technique dûment valorisé dans une économie numérique tirée par une croissance spectaculaire. Et si la période est bien sûr à l'expérimentation du potentiel démocratique

à des mesures urgentes et exceptionnelles pour gérer cette menace » (Buzan et Wæver 2003, 491)

d'Internet, le niveau de transgression semble être redescendu de plusieurs crans, le « web militant » se structurant essentiellement autour de modes d'action expressiviste ou légaliste.

Certes, les états-majors des agences de sécurité affirment toujours redouter l'avènement d'un nouveau type de conflit propre aux réseaux informatiques – la *netwar* ou « guerre en réseau » –, menée notamment par des acteurs non-étatiques dotés d'organisations horizontales, transnationales et sans leaders clairement identifiables (Arquilla et Ronfeld 2001). Mais ces discours semblent surtout conçus pour justifier l'institutionnalisation des vieilles stratégies contre-insurrectionnelles envers des groupes suspects de vouloir perturber l'infrastructure informatique, et engager le démantèlement de certaines protections juridiques associées à l'État de droit pour agir avec davantage de célérité et d'efficacité contre ces illégalismes politiques propres au cyberespace (Jones 2017).

D'ailleurs, par la suite, chaque fois qu'un « front hacker » menace de se reformer, ses acteurs sont de nouveau confrontés à ces stratégies. À la fin des années 1990, tandis que l'altermondialisme tente de remettre au goût du jour les répertoires d'action hacktivistes en les présentant comme des formes de désobéissance civile – avec notamment des attaques « en déni de service »[7] destinées à ralentir momentanément des sites web (actions présentées comme l'équivalent numérique des *sit-ins*), de nouvelles fuites de documents, des campagnes de *mail-bombing*, etc. –, les États engagent des adaptations législatives qui les autorisent à réprimer ces agissements en mobilisant les dispositifs antiterroristes (Manion et Goodrum 2000, Tréguer 2019). De même, vers 2010, lorsque WikiLeaks fait son entrée fracassante sur la scène géopolitique mondiale en publiant les documents fuités par l'analyste militaire Chelsea Manning et que la mouvance Anonymous tente de remettre sur le devant de la scène les tactiques hacktivistes, les États mobiliseront de nouveau avec succès l'approche répressive inaugurée au tournant des années 1980, désormais agrémentée de l'arsenal constitué depuis 2001 dans le cadre de la lutte antiterroriste (Sauter 2014).

Conclusion

Rétrospectivement, la répression des hackers au tournant des années 1980 semble donc pouvoir s'interpréter comme l'un des fronts d'une stratégie plus large visant à disqualifier les répertoires d'action transgressifs, *a fortiori* dès lors qu'ils prennent pour cible une infrastructure numérique devenue critique.

[7] Une attaque par « déni de service » (ou « attaque DoS » pour « Denial of Service ») consiste à rendre indisponible un service en ligne, par exemple en cherchant à saturer le serveur qui l'héberge en lui envoyant un très grand nombre de requêtes de connexion.

De ce point de vue, les pratiques hacktivistes paraissent avoir fait les frais de « l'inflation d'un moralisme anti-violence » décrite par la philosophe Mathilde Girard, ce « discrédit de tout ce qui, du domaine des conduites individuelles comme des pratiques politiques, relève de la violence », même symbolique (Girard 2010). Sans même parler du sabotage informatique qui bénéficiait jusqu'au milieu des années 1980 d'une relative mansuétude de la part des autorités – la police qualifiait encore les actes incendiaires du CLODO « d'actions non-violentes » (Izoard 2010, 265) –, le simple fait de contribuer à faire fuiter des documents d'intérêt public expose aujourd'hui les hackers à des sanctions exemplaires, comme l'illustre le sort réservé à Julian Assange ou le cas du jeune militant anarchiste Jeremy Hammond, reconnu coupable de la fuite de courriels d'une agence de renseignement privée et condamné en novembre 2013 à dix ans de prison ferme[8]. En France, les bénignes attaques en déni de service conduites ces dernières années par des hackers et militants écologistes ont fait l'objet d'un traitement policier et judiciaire disproportionné, mobilisant les services de renseignement intérieurs et des techniques d'enquête spéciales (Tréguer 2015). Les cas d'infiltrations, le recrutement d'informateurs, voire de surveillance ou de censure extra-légales contre des groupes hacktivistes en passe de s'organiser sont encore régulièrement recensés.

Même en faisant abstraction des risques politiques associés aux procès en illégitimité et au coût de la répression, l'évolution de l'économie politique de l'informatique s'est aussi passablement transformée : si les illégalismes hackers étaient apparus dans un contexte où quelques militants isolés mais compétents et motivés pouvaient encore tenir en échec les infrastructures de puissantes organisations, celles-ci ont depuis largement renforcé la « cybersécurité » de leurs actifs stratégiques, limitant les occasions tactiques offertes aux hackers militants.

L'espace juridico-politique et les possibilités socio-techniques qui, historiquement, sous-tendaient les logiques d'action directe transgressive dirigées contre l'informatique dominante semblent donc réduits à une portion congrue. La lutte contre les sociétés de contrôle paraît désormais enfermée dans des répertoires d'action conventionnels et souvent légalistes, dont l'efficacité s'avère en pratique limitée. Au-delà des seuls hacktivistes – et malgré les mobilisations parfois puissantes qui, à l'image des Gilets Jaunes en France, émaillent l'actualité et qui s'exposent elles aussi à la répression –, l'intelligence tactique, la radicalité politique et les ressources d'action collective dont disposaient les groupes associés à la Nouvelle Gauche dans leur opposition à l'ordre technocratique se sont globalement taries. L'informatique de contrôle prolifère mais pour l'heure, au prix d'une consolidation

[8]Hammond est finalement sorti de prison en novembre 2020, après plus de huit années d'incarcération.

des fondements autoritaires du libéralisme, les défenseurs de la société de contrôle semblent parvenus à contenir toute nouvelle crise susceptible de la menacer.

Bibliographie

Arquilla, J., & Ronfeldt, D. F. (Éds.). (2001). *Networks and Netwars*. Rand Corporation.

Beltramini, E. (2020). Against technocratic authoritarianism. A short intellectual history of the cypherpunk movement. *Internet Histories*, *0*(0), 1-19.

Bequai, A. (1987). *Technocrimes : The Computerization of Crime and Terrorism*. Lexington Books.

Bey, H. (2003). *T.A.Z. the Temporary Autonomous Zone, Ontological Anarchy, Poetic Terrorism* (2e éd.). Autonomedia.

Borland, J. (2013, décembre 29). WikiLeaks' Assange : Sysadmins of the World, Unite ! *Wired*. https://www.wired.com/2013/12/wikileaks-assange-sysadmins-world-unite/

Breton, P., Heilmann, E., & Bertrand, I. (1991). Entre l'ordre et le désordre, les valeurs paradoxales du monde de l'informatique. *Réseaux*, *9*(48), 13-22.

Brigades rouges. (1980, décembre). Les vingt thèses finales (17-18). *L'ape e il Comunista*, *16-17*.

Buzan, B., & Wæver, O. (2003). *Regions and Powers : The Structure of International Security*. Cambridge University Press.

Cardon, D., & Granjon, F. (2010). *Médiactivistes*. Les Presses de Sciences Po.

Certeau, M. de. (1990). *L'invention du quotidien, tome 1 : Arts de faire* (Nouv. éd.). Gallimard.

Chamayou, Gregoire. (2018). *La Société ingouvernable : Une généalogie du libéralisme autoritaire*. La Fabrique.

Chamayou, Grégoire (Éd.). (2020). *Du libéralisme autoritaire*. La Découverte.

Coleman, G. (2012). Phreaks, Hacker, and Trolls : The Politics of Transgression and Spectacle. In *The Social Media Reader*. New York University Press.

Corrigan-Gibbs, H. (2014). Keeping Secrets. *Stanford Magazine*, (novembre 2014).

Crozier, M., Huntington, S. P., & Watanuki, J. (1975). *The Crisis of Democracy : Report on the Governability of Democracies to the Trilateral Commission*. New York University Press.

Deleuze, G. (1990). Post-scriptum sur les sociétés de contrôle. *L'Autre journal*, *1*.

Duff, L., & Gardiner, S. (1996). Computer Crime in the Global Village : Strategies for Control and Regulation — in Defence of the Hacker. *International Journal of the Sociology of Law*, *24*(2), 211-228.

Feenberg, A. (2004). *Repenser la technique : Vers une technologie démocratique*. La Découverte.

Foucault, M. (1997). *« Il faut défendre la société » : Cours au Collège de France, 1976*. Seuil.

Foucault, M. (2004). *La Naissance de la biopolitique. Cours au Collège de France, 1979*. Le Seuil.

Girard, M. (2010). Du dedans au dehors de l'espace démocratique : La désobéissance civile. *Multitudes*, *41*(2), 212.

Gros, F. (2010). Foucault et « la société punitive ». *Pouvoirs*, *135*(4), 5-14.

Guisnel, J. (1995). *Guerres dans le cyberespace : Services secrets et Internet*. La Découverte.

Izoard, C. (2010). L'informatisation, entre mises à feu et résignation. In C. Biagini & G. Carnino (Éds.), *Les Luddites en France : Résistances à l'industrialisation et à l'informatisation* (p. 251-286). Editions L'échappée.

Jones, M. L. (2017). The spy who pwned me. *Limn*, *8*.

Kraft, P. (1977). *Programmers and Managers : The Routinization of Computer Programming in the United States*. Springer.

Lefebvre, H. (1967). *Position : Contre les technocrates*. Gonthier.

Levine, Y. (2018). *Surveillance Valley : The Secret Military History of the Internet*. PublicAffairs.

Lunceford, B. (2009). Building Hacker Collective Identity One Text Phile at a Time : Reading Phrack. *Media History Monographs*, *11*(2).

Manion, M., & Goodrum, A. (2000). Terrorism or Civil Disobedience : Toward a Hacktivist Ethic. *SIGCAS Computer & Society*, *30*, 14-19.

Nissenbaum, H. (2004). Hackers and the contested ontology of cyberspace. *New Media & Society*, *6*(2), 195-217.

Ross, A. (1990). Hacking Away at the Counterculture. *Postmodern Culture*, *1*(1).

Sauter, M. (2014). *The Coming Swarm : DDOS Actions, Hacktivism, and Civil Disobedience on the Internet*. Bloomsbury Academic.

SDS. (1962, juin). *Port Huron Statement of the Students for a Democratic Society*. Documents for the Study of American History.

Sterling, B. (1993). *The Hacker Crackdown : Law And Disorder On The Electronic Frontier*. Bantam.

Thomas, J. (2005). The moral ambiguity of social control in cyberspace : A retro-assessment of the 'golden age' of hacking. *New Media & Society*, *7*(5), 599-624.

Thyraud, J. (1987). *Rapport sur la proposition de loi adoptée par l'Assemblée nationale relative à la fraude informatique* (No 3). Sénat.

Tréguer, F. (2015). Le droit pénal de la fraude informatique, nouvel ami des censeurs ? *La Revue des droits de l'homme - Actualités Droits-Libertés*.

Tréguer, F. (2019). *L'utopie déchue : Une contre-histoire d'Internet, XV^{è}-XXI^{è} siècle*. Fayard.

Turner, F. (2012). *Aux sources de l'utopie numérique : De la contre-culture à la cyberculture, Stewart Brand, un homme d'infliuence* (L. Vannini, Trad.). C&F éd.

Vaneigem, R. (1992). *Traité de savoir-vivre à l'usage des jeunes générations* (2e éd.). Gallimard.