Congrès AFSP Bordeaux 2019

ST 59 : Politiques du hacking. Enquête sur les ruses numériques

Résister aux sociétés de contrôle, subvertir l'informatique dominante : une typologie des illégalismes hackers[1]

Félix Tréguer (CERI Sciences Po)
felix.treguer at sciencespo.fr

Résumé :

Dans les années 1980 et 1990, alors que les premiers réseaux informatiques ouverts au public se développent en Europe et en Amérique du Nord, une élite militante émerge au sein des milieux informaticiens : les hackers. Du Chaos Computer Club en Allemagne aux médiactivistes italiens en passant par les incendiaires français du *Comité pour la Libération ou le Détournement des Ordinateurs* (CLODO), le point commun de ces divers acteurs dotés d'un fort capital technique est l'opposition au modèle dominant d'informatisation au travers de pratiques de sabotage, de destruction ou de détournement. Avec leurs illégalismes, les hackers apparaissent ainsi comme les « lanceurs d'alerte » de la société en réseau, pointant les vulnérabilités techniques de ce nouveau macro-système technique, ainsi que ses effets politiques délétères, en esquissant aussi le plus souvent des appropriations alternatives en liant avec les mouvements sociaux auxquels ils s'allient.

Derrière une identité « hacker » partagée se cache cependant une une multiplicité de trajectoires militantes et de rapports à l'informatique, oscillant entre postures néo-luddites et projets émancipateurs relevant d'une « technophilie critique ». À partir de classiques des *hacker studies* et de sources secondaires émergentes complétées par certaines archives, cette communication propose ainsi une typologie des illégalismes initiés par la mouvance hacker à partir des années 1980 pour résister aux « sociétés de contrôle » de l'ère numérique. Après un rapide état des lieux sur l'historiographie de la mouvance et ses limites, nous proposons d'élargir la focale pour recenser les différentes modalités de sabotage et de subversion de l'informatique connectée élaborées et expérimentés par ces acteurs militants. Plutôt que de rechercher l'exhaustivité, nous retenons pour chacun de ces modes d'action un moment de genèse, de cristallisation, ou des incarnations paradigmatiques. En conclusion, nous revenons sur certains débats stratégiques au sein de la mouvance et la répression croissante de ces illégalismes hackers. Une répression qui, en lien avec les changements intervenus dans l'économie politique d'Internet, semble avoir refermé la structure d'opportunité qui avait permis leur genèse.

1. Texte non achevé présenté au 15è Congrès de l'AFSP le 2 juillet 2019.

Introduction

Au tournant des années 1980, Gilles Deleuze propose une analyse visionnaires des « sociétés de contrôle » propres au cycle politique ouvert dans les années 1970, et que certains sociologues et technocrates avaient eu tôt fait de qualifier de « post-industrielles ». Dans une conférence de 1987 à la Femis, puis dans un entretien avec Toni Negri et un court texte paru en 1990 (Deleuze, 1990), le philosophe introduit ce concept dans le but de prolonger les analyses de Michel Foucault sur les régimes d'économie politique du pouvoir.

Pour Deleuze, la gouvernementalité prend désormais des apparences moins autoritaires, plus souples et plus « économes ». Dans la « société de contrôle », qui coexiste avec les châtiments exemplaires propre aux sociétés de souveraineté de l'ère féodale et avec les logiques disciplinaires des régimes libéraux (Razac, 2008), la domination s'exerce en milieux ouvert : il ne s'agit plus tant de discipliner les sujet que de gérer les flux de population et de production, pris dans leur « naturalité ». Deleuze estime ainsi que 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).

Faisant écho aux critiques de l'informatique qui avaient fait florès à partir de la fin des années 1960, Deleuze repérait déjà l'importance de l'ordinateur et des réseaux informatiques, véritables clés de voûte de ce nouveau régime de domination :

> « Il n'y a pas besoin de science-fiction, écrit le philosophe, pour concevoir un mécanisme de contrôle qui donne à chaque instant la position d'un élément en milieu ouvert, animal dans une réserve, homme dans une entreprise (collier électronique) (…) Ce qui compte n'est pas la barrière, mais l'ordinateur qui repère la position de chacun, licite ou illicite, et opère une modulation universelle ».

Trente ans plus tard, la science fiction est en effet inutile. À l'heure des controverses sur le capitalisme de surveillance, les « fake news », la montée en puissance des théories du *nudge* et de l'économie comportementale, ou sur les systèmes de réputation ou « crédit social » expérimentés par certaines entreprises où même des États comme la Chine, les manifestations de la société de contrôle semblent toujours plus nombreuses. Et si elles reposent en effet sur l'informatique en réseau, ce n'est pas tant que la technologie détermine les formes du contrôle social. D'après Deleuze, c'est plutôt que les machines propres à chaque époque « expriment les formes sociales capables de leur donner naissance et de s'en servir ». Certes, écrit-il, l'ordinateur et les modalités de contrôle social auxquelles il participe sont particulièrement complexes et diffuses. Pour autant, « 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, dit-il, c'est « chercher de nouvelles armes ». Or, la complexité croissante des machines qui sous-tendent les différents régimes de pouvoir constitue aussi leur point 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 au tournant des années 1980, le personnage du « pirate informatique » et la mouvance hacker se sont imposés dans les imaginaires comme l'archétype de la subversion numérique. Certains de ses *illégalismes* – un terme utilisé par Foucault pour désigner « l'ensemble des pratiques qui soit transgressent délibérément, soit contournent ou même détournent la loi » (Gros, 2010)– font les gros titres depuis quelques années. Dans cet

article, nous voudrions prolonger la réflexion du philosophe en portant l'attention sur les modes de résistance aux sociétés de contrôle portés par les hackers. Après un rapide état des lieux sur l'historiographie de la mouvance et ses limites, nous proposons d'élargir la focale pour recenser les différentes formes de sabotage et de subversion de l'informatique connectée élaborées et expérimentées par des acteurs militants qui y sont associés. Plutôt que de rechercher l'exhaustivité, nous retenons pour chacun de ces modes d'action un moment de genèse, de cristallisation, ou des incarnations paradigmatiques. En conclusion, nous reviendrons sur certains débats stratégiques interne à la mouvance sur ces répertoires d'action, et sur les effets politiques de ces illégalismes exposés à la répression.

1. La mouvance hacker : figure de proue de l'activisme numérique

La mouvance hacker constitue à bien des égards une figure fondatrice de l'« activisme numérique », terme qui renvoie à la myriade d'acteurs doublement engagés non seulement *par* mais surtout *pour* des usages émancipateurs de l'informatique connectée, faisant de l'infrastructure numérique l'objet d'une lutte politique. Le mot lui-même est apparu dans les milieu d'étudiants en informatique du Massachusetts Institute of Technology (MIT) aux États-Unis, d'abord sous la forme d'un verbe – *to hack* – désignant un bricolage inventif, une solution technique ingénieuse. Dans les années 1960 et 1970, il se répand rapidement dans les cercles de passionnés d'informatique et le mot « hacker » en vient à désigner un virtuose du code informatique, doué d'une grande habilité dans sa capacité à détourner un système technique, à contourner les contraintes, à répondre à un problème en se déprenant des méthodes conventionnelles.

Dans les années 1980, alors que l'informatique connectée arrive dans les foyers les plus privilégiés, le terme prend un sens plus politique, notamment sous l'influence du livre *Hackers*, publié par le journaliste Steven Levy en 1984 et qui demeure aujourd'hui encore une référence. Le journaliste met en évidence l'influence de la contre-culture des années 1960 sur la mouvance, le rapport compliqué à l'autorité au sein de ce milieu, et l'exigence de justice qui s'en dégage. Lorsqu'il se propose d'expliciter les axiomes d'une « éthique hacker », l'auteur insiste sur leur croyance dans les vertus émancipatrices de l'informatique et de l'accès à l'information, leur profond attachement à la méritocratie, au « faire », mais aussi leur méfiance exacerbée envers l'autorité qu'ils cherchent à entraver en distribuant le pouvoir au travers d'architectures socio-techniques décentralisées (Levy, 1984). Mais c'est aussi l'époque ou le hacker fait l'objet de cadrages négatifs et devient associé à la criminalité informatique, à une époque ou les réseaux connectés sont en proie à un intense processus de sécurisation.

Les hackers constituent aujourd'hui encore une nébuleuse particulièrement diverse, tant en termes de pratiques que d'idéologies politiques. Tant et si bien qu'il faudrait sans doute davantage parler du *hacking* (comme pratique) que des *hackers* (comme groupe social). Tous, loin de là, n'adhèrent pas aux visées émancipatrices et aux pratiques politiques subversives des membres les plus engagés dans l'activisme numérique. Tim Jordan et Paul Taylor rappellent ainsi que nombre d'individus socialisés au sein de ces communautés techniciennes font le choix de travailler pour les grandes multinationales de l'économie numérique, de la finance, ou au service des agences de police et de renseignement (Jordan et Taylor, 2004). À cette récupération des hackers par le capitalisme informationnel et l'État s'ajoute la cooptation de ceux qu'on désigne comme des « *black hats* » par les réseaux mafieux et criminels (Jordan, 2013). L'anthropologue Gabriella Coleman, spécialiste des mouvements du logiciel libre et de la culture hacker, souligne elle aussi le caractère éminemment complexe et parfois contradictoire des différentes branches de la mouvance, tout en rappelant qu'ils ont tendance à s'accorder sur des valeurs libérales (« liberté, vie privée, accès »), leur « adoration » de l'informatique et des réseaux de communication, et leur

position généralement privilégiée dans le champ économique lucratif de la programmation informatique (Coleman, 2014a).

En abordant la question des formes de subversion et de sabotage visant les réseaux numériques expérimentés par la mouvance hacker à travers son histoire, nous aimerions à la fois prolonger les analyses anciennes sur les liens entre les hackers politiques et les mouvements sociaux (Costanza-Chock, 2003 ; Blondeau, 2007 ; Dominguez, 2009), tout en intégrant certains acteurs ayant jusqu'ici échappé à l'historiographie dominante. Dans la lignée de travaux récents (e.g. Maxigas, 2017), il s'agit notamment d'intégrer des militants relevant de cette étiquette sans forcément la revendiquer, et qui soient non seulement opposés aux trajectoires techno-scientifiques dominantes mais qui, de manière plus tranchée encore, aient assumé une posture *technocritique* en cherchant à déconstruire l'idée que « le progrès des machines est un progrès vers la liberté, vers l'égalité, vers la concorde » (Jarrige, 2016). En bref, s'ils correspondent à la définition classique des hackers par leur important capital technique, leur esprit frondeur ou leurs tactiques rusées et ingénieuses, ces acteurs issus des marges de la mouvance hacker s'en écartent on le verra par leur critique située et radicale de l'informatique.

Outre cette frange technocritique radicale, nous tentons également de mobiliser des sources éparses et des travaux récents sur les hackers européens – encore largement négligés dans l'historiographie dominante – afin de montrer à la fois la diversité des pratiques subversives liées à la mouvance, les formes de synchronie ou de circulation des modes d'action à travers le temps et l'espace. Nous adoptons une approche là encore relativement large des formes de sabotage et de subversion, en nous intéressant non seulement à ceux qui prennent pour objet les ordinateurs et les réseaux en tant que tels, mais aussi leurs usages dominants (notamment médiatiques). Tout en restant attentif aux articulations entre différents répertoires d'actions, nous laisserons de côté ceux qui ne transgressent pas les formes traditionnelles et prescrites de l'engagement et du conflit politique, en particulier lorsqu'ils relèvent du droit (soit qu'il s'agisse de porter un plaidoyer institutionnel devant le législateur ou les tribunaux pour défendre les droits fondamentaux, soit que le droit serve à la création de nouvelles institutions capables de protéger ces mêmes valeurs, comme l'illustre le mouvement du logiciel libre).

2. Diversité des modes de subversion des sociétés de contrôle

a. Dénoncer les failles de sécurité

Le premier mode d'action à considérer est héritier de l'art du *phreaking* – néologisme issu de la contraction des termes « *phone* » et « *freak* » qui désigne les pratiques techniques permettant l'utilisation gratuite et le détournement du réseau téléphonique des grands opérateurs télécoms à des fins souvent potaches (Coleman, 2012). Transposé à l'informatique, le phreaking consiste notamment à exploiter des vulnérabilités – ou failles informatiques – afin de pénétrer sur des systèmes informatiques distants et d'utiliser ces accès non-autorisés à des fins stratégiques, par exemple pour dénoncer les risques que ces systèmes font peser sur la vie privée.

L'un des premiers faits d'armes en la matière est probablement le « hack » fondateur du Chaos Computer Club (CCC), fondé en 1981 par Wau Holland (Bowcott et Hamilton, 1990 ; Wieckmann, 1989 ; Denker, 2014). Holland a baigné dans les mouvements de la contre-culture allemande. Né à Cassel, dans le nord-ouest de l'Allemagne en 1951, il a étudié le génie électrique, l'informatique et les sciences politiques à l'université. Lecteur de Marx, il s'adonne aussi au phreaking dans les années 1970, dénichant une faille dans le réseau de Deutsche Telekom qui permet de passer des appels nationaux au prix des appels locaux. Après ses études, il travaille pour des libraires engagés à gauche, avant de rejoindre une petite entreprise de développeurs. À

l'époque, la gauche allemande oscille entre le technocratisme des communistes, favorables aux grands projets productivistes, tandis qu'anarchistes et écologistes campent encore sur une position d'opposition radicale à la technologie (au milieu des années 1980, le groupe des Verts au Bundestag refusera par exemple de prendre part au plan d'informatisation du travail parlementaire). Holland, lui, partage une partie des thèses hostiles à l'informatique, dont il comprend qu'elle est une arme au service des dominants (Denker, 2014). Mais il est aussi convaincu que l'informatique personnelle, en décentralisant la ressource informatique, peut permettre une appropriation subversive de ces machines, notamment dans le but de développer des usages médiatiques émancipateurs.

À travers une tribune publiée en 1981 dans un journal, Holland lance un appel à tous ceux qui se retrouvent dans ses analyses, avec l'idée d'imiter ce qui se fait aux États-Unis où le milieu hacker commence tout juste à se structurer. Une revue alternative est bientôt lancée pour échanger des informations sur les vulnérabilités informatiques, des moyens de détourner les ordinateurs, mais aussi des articles sur les plans du gouvernement en vue d'interrompre toutes les télécommunications en cas de guerre ou de catastrophe naturelle. Chez Holland et le reste du mouvement hacker allemand, Orwell et son Big Brother sont une référence fondamentale. Aussi le CCC se donne-t-il pour rôle de fédérer l'avant-garde hacker afin de sensibiliser l'ensemble de la population aux risques que fait peser l'informatique pour les libertés publiques, le tout sans se départir d'une bonne dose d'humour.

Dans ces premiers années, les actions du CCC consistent notamment à tourner en ridicule l'équivalent allemand du Minitel, le BTX. En 1984, avec son acolyte Steffen Wernéry qui exerce avec lui le rôle de porte-parole du mouvement, Holland signe le premier grand hack public du CCC. Ce jour-là, les deux compères tiennent une conférence de presse à laquelle ils convient le responsable de la CNIL locale, et au cours de laquelle ils vont revendiquer rien de moins que le « braquage d'une banque ». La veille, expliquent-ils aux journalistes, ils ont exploité une faille leur permettant de découvrir le mot de passe du compte BTX de la caisse d'épargne de Hambourg, réussissant ainsi à virer 135 000 deutsche mark sur leur propre compte bancaire. Holland racontera plus tard comment lui et Wernéry s'étaient mis d'accord sur la somme à subtiliser : « En moyenne, un braquage dans une banque rapporte environ 10 000 deutsche mark. Pour que cela soit pertinent du point de vue de l'opinion publique, il fallait que cela soit multiplié par dix » (Georgen, 2014). Pour récupérer l'argent, ils ont écrit un petit programme permettant d'appeler automatiquement la page BTX du CCC chaque fois qu'ils pressent sur la touche dièse de leur poste BTX, chaque consultation de la page étant facturée 9,97 deutsche mark prélevés directement sur le compte de la banque. Suite à la conférence de presse, alors relayée par tous les grands médias allemands, l'argent sera restitué sans que la banque ne porte plainte, et les postes allemandes seront sommées de réparer cette embarrassante faille au plus vite.

Ce hack fondateur permet de sceller l'identité du CCC, décrit quelques années plus tard par Wernéry comme « un groupe de passionnés d'informatique qui ont choisi de se comporter de façon créatrice, pratique et irrespectueuse face à la technique, et de dénoncer les failles des systèmes afin de permettre aux utilisateurs de mieux s'en protéger » (1989). Très tôt, les leaders du Club tentent également de faire admettre aux militants technocritiques ou aux élus écologistes du Bundestag la possibilité d'une informatique alternative et émancipatrice, sans grand succès au départ puisque l'hostilité à l'endroit de ces machines domine encore la Nouvelle Gauche allemande. En 1985, un obscur groupe baptisé « Black & White against the Computer State », les accuse même d'être les idiots utiles de l'industrie informatique (Denker, 2014). En quelques années à peine, grâce à ses actions de communication et de sensibilisation (notamment son congrès annuel qui, dès 1984, réunit près de 400 participants à Hambourg), il devient une institution respectée dans les milieux d'informaticiens et de militants de la vie privée. Il entre

même en contact avec des acteurs institutionnels en charge de la protection des données personnelles. Il deviendra un modèle pour d'autres groupes hackers en Europe.

b. Brouillage et destructions des systèmes informatiques

Si le fait d'exploiter une faille de sécurité aux seules fins de dénonciation et d'alerte tombe déjà en théorie sous le coup des infractions associées à la fraude informatique adoptées dans les pays occidentaux à la fin des années 1980, les formes de brouillages et de destructions auxquelles Deleuze semble faire référence vont un cran plus loin dans la transgression. Dès les années 1980, la possibilité de pénétrer illégalement dans les systèmes informatiques de l'armée, du gouvernement ou de grandes entreprises laisse ainsi entrevoir la possibilité de nouveaux modes d'action. Fort de leur supériorité technique, les hackers en viennent ainsi à penser l'ordinateur comme une arme de lutte, et le l'espace de communication formé par les réseaux informatiques comme terrain de bataille. Ainsi, pour Gareth Branwyn, un journaliste qui prend part aux communautés hackers 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).

Ces approches semblent en fait directement inspirées par une vague d'« actions directes » de groupes d'extrême gauche qui, depuis la fin des années 1960, dénoncent l'informatisation et son inféodation aux logiques capitalistes et militaires à travers la destruction physique d'équipements informatiques (incendies ou explosifs) (Tréguer, 2019a). Une illustration qui semble pouvoir être rapprochée de la mouvance hacker est fournie par un groupe français : le Comité liquidant ou détournant les ordinateurs, ou CLODO. Entre 1980 et 1983, ce collectif non-identifié défraie la chronique au gré d'une série d'actions spectaculaires dans la région de Toulouse, haut lieu de l'industrie informatique française (Izoard, 2010). Tout commence la nuit du 5 avril 1980, lorsque les installations de la société Phillips Informatique sont l'objet d'un violent incendie. La *Dépêche du Midi* parle alors d'un « sabotage d'artistes » :

> « Les ordinateurs ont été mis hors d'état de nuire sans même être égratignés. Des disques cassettes, des fiches entièrement brûlées dans les toilettes de l'entreprise, n'ont laissé qu'une odeur diffuse et des cendres sur le sol ».

Les dégâts sont estimés à près de deux millions de francs. Le même *modus operandi* est reproduit trois jours plus tard dans les locaux de la société CII-Honeywell-Bull, puis le 20 mai chez un autre constructeur informatique, International Computers Limited. En septembre suivant, c'est à la société de service informatique CAP-SOGETI d'en faire les frais. Le CLODO se fait oublier pour un temps. Alors que l'ordinateur personnel commence à gagner du terrain et que la presse s'enthousiasme alors pour la « révolution informatique », le groupe revient avec ce qui restera comme son action la plus spectaculaire. Le 28 janvier 1983, en pleine nuit, le centre informatique de la préfecture de Haute-Garonne est soufflé par quatre charges d'explosifs. Les dégâts sont estimés à 30 millions de francs. Les policiers venus constater les dégâts feront l'hypothèse que les auteurs de l'attentat étaient familiers des lieux. Avec cet attentat, le groupe attire l'attention de la CIA, qui en fait mention dans dans son rapport périodique intitulé « Terrorism Review » (1983).

Dès le début, le CLODO revendique ses actions. Après son incendie inaugural en avril 1980 – et alors que les observateurs suspectent un temps l'implication du groupe d'extrême-gauche Action directe –, un communiqué de presse est diffusé par le collectif et relayé dans les journaux :

> « Nous sommes des travailleurs de l'informatique, bien placés pour connaître les dangers actuels et futurs de l'informatique et de la télématique. L'ordinateur est l'outil préféré des dominants. Il sert à exploiter, à ficher, à contrôler et à réprimer ».

Travailleurs de l'informatique, usant de l'humour et de la dérision, contournant les mesures de sécurité des établissements industriels pour mener à bien leurs actions (notamment à travers le crochetage de serrures, un art prisé dans le milieu), les membres du CLODO ne se revendiquent pas hackers mais correspondent pour partie à la définition. Comme l'explique Celia Izoard, leur action « est tissée dans celle, plus large, du mouvement anarchiste libertaire toulousain de l'époque, qui choisit soigneusement ses cibles et multiplie les canulars sans faire de victime », notamment dans le cadre de campagnes contre le fichage ou l'énergie nucléaire. Au-delà du clin d'œil au mouvement situationniste, la référence au détournement dans l'acronyme du groupe laisse entendre que, dans un autre monde, avec d'autres rapports de pouvoir, une informatique émancipatrice reste envisageable. Pour l'heure, le CLODO voit dans l'ordinateur « le serviteur zélé du système dans lequel nous vivons », un outil « sans doute perverti par ses origines mêmes », et notamment « l'abus du quantitatif ou la réduction au binaire » :

> « Il faut bien que la vérité de cette informatisation soit parfois démasquée, qu'il soit dit qu'un ordinateur n'est qu'un tas de ferraille qui ne sert qu'à ce que l'on veut qu'il serve, que dans notre monde il n'est qu'un outil de plus, particulièrement performant, au service des dominants (…) : mise en fiches, surveillance par badge et cartes, instrument de profit maximalisé pour les patrons et de paupérisation accélérée pour les rejetés. »

Comme le rappelle Izoard, l'enjeu du sabotage est à l'époque également évoqué dans la presse française et par certains syndicats comme un mode d'action politique légitime.

On retrouve des préoccupations similaires aux États-Unis dans Processed World, un fanzine lancé en 1981 dans la région de San Francisco et actif durant toute la décennie (Carlsson, 1990 ; Wright, 2011), et qui traduira et republiera d'ailleurs l'une des interview du CLODO (d'abord parue en français dans la revue de critique de l'informatique *Terminal*). Alors que l'informatisation déferle sur la société américaine, ce périodique donne la voix à de jeunes diplômés qui ont appris les rudiments d'informatique à l'université et trouvent alors à s'embaucher comme employés de bureau dans un secteur tertiaire en pleine expansion. À travers leurs textes, leurs poèmes ou leurs détournements graphiques souvent plein d'humour et, à l'image du CLODO également inspirés par le Situationnisme, les contributeurs de Processed World proposent des analyses acerbes de la vie de bureau, du profond ennui et parfois de la colère que leur inspire cet univers de travail aseptisé. Ces considérations les amènent naturellement à envisager la question du sabotage de leurs outils de travail.

c. Fuite d'actifs informationnels

Troisième catégorie de mode de subversion des réseaux informatiques dominants : l'accès et la diffusion sur Internet d'informations que les grandes instituions voudraient garder secrètes ou qu'elles tentent de censurer. Dans les années 1970, les fuites d'informations secrètes se sont ancrées dans les répertoires d'action des mouvements contestataires, comme l'illustrent des épisodes comme de COINTELPRO ou des Pentagon Papers aux États-Unis, ou de la lutte contre la militarisation du plateau du Larzac en France. Dès les années 1980, des hackers militants de la cryptographie en viennent aussi à concevoir ces techniques de chiffrement comme une manière de faciliter ce répertoire d'action, en assurant l'anonymat et la confidentialité des communications, pour ainsi faire fuiter des documents d'intérêt public et réduire le risque d'être repéré et poursuivi (Levy, 2001 ; Greenberg, 2012 ; Myers West, 2017).

L'exemple le plus retentissant de ce mode d'action demeure la série de fuites orchestrées par WikiLeaks en 2010, qui diffuse cette année-là des informations transmises par la lanceuse d'alerte Chelsea Manning sur les conflits militaires en Irak et en Afghanistan, ainsi que des millions de câbles diplomatiques américains (un épisode resté dans les mémoires comme le Cablegate). Julian Assange, le fondateur de WikiLeaks est héritier de la mouvance « cypherpunks », un groupe dont

il fréquente la *mailing list* éponyme au début des années 1980. Il aussi fait partie d'un groupe hacker appelé les *International Subversives*, visés par plusieurs enquêtes au tournant des années 1980 pour avoir pénétré les réseaux du complexe militaro-industriel occidental (Dreyfus et Assange, 2012). Dans l'essai intitulé *State and Terrorist Conspiracies* (Assange, 2006), il livrait déjà son programme politique. Il y décrit les États comme des réseaux d'information entre différents acteurs (appelés « agents » ou « institutions »), réagissant aux informations présentes dans leur environnement et collaborant en vue d'une même fin. Or, toute organisation de ce type qui verserait dans l'abus de pouvoir cherche nécessairement à dissimuler les échanges d'informations en son sein afin de minimiser le risque de résistance à la domination qu'elle exerce. Dans ce cadre analytique, la fuite d'informations doit donc permettre de rompre les échanges secrets d'information et de créer autant de dysfonctionnements capable de ralentir et, *in fine*, de déjouer cette conspiration.

En 2010, l'émergence tonitruante de WikiLeaks sur la scène géopolitique internationale va ainsi catalyser un répertoire d'action issu de la mouvance hacker qui, depuis les années 1980, était tombé en déshérence : les « hacks d'intérêt public » ou, autrement dit, l'accès non-autorisé à des données informatiques dans le but d'obtenir des informations d'intérêt public et de les publier (Coleman, 2017)[2]. Début 2011, à la suite du Cablegate, la mouvance Anonymous qui a apporté son soutien à WikiLeaks, devient un objet d'attention pour de nombreuses agences de police et de renseignement. L'un des dirigeants de la firme texane HBGary), spécialiste de sécurité informatique, entreprend alors d'identifier certains des leaders de la mouvance, histoire de montrer le savoir-faire de l'entreprise auprès de ses pairs. En surveillant en simultané l'un des salons IRC du groupe et son activité sur Twitter, il identifie plusieurs comptes, et prétend au bout de quelques semaines être en mesure de donner les pseudonymes et lieux de résidence de certains membres. Pour se faire un peu de publicité à bon compte, il décide de rendre cette information publique, et accorde une interview au Wall Street Journal qui publie un article sur le sujet. C'est alors qu'une branche des Anonymous, qui plus tard se fera connaître sous le nom de Lulzsec, décide de représailles : ils découvrent une faille de sécurité dans les serveurs d'HBGary et copient plusieurs dizaines de milliers de documents, dont des courriers électroniques internes compromettants. Ces documents, fuités sur le site AnonLeaks.org en février 2011, vont révéler le projet « Team Themis » : HBGary, Palantir et d'autres entreprises de sécurité proches du Pentagone ont été employées par Bank of America et la Chambre de Commerce des États-Unis pour établir une stratégie et des méthodes d'infiltration visant à nuire à la réputation de WikiLeaks et de certains de ses soutiens dans les médias, comme le journaliste Glenn Greenwald. Au final, c'est bien HBGary qui verra sa réputation ruinée par ces fuites, qui conduiront d'ailleurs le Congrès américain à lancer deux commissions d'enquêtes contre elle.

Une autre fuite retentissante est revendiquée par des hackers d'Anonymous début 2012. WikiLeaks annonce alors être en possession de près de 5 millions de mails internes de l'entreprise Stratfor, une société américaine de renseignement et d'analyse géopolitique qui entretient elle aussi des liens nourris avec le Pentagone. L'ensemble a été transmis par un militant anarchiste opérant sous la bannière d'Anonymous, Jeremy Hammond. Durant toute l'année 2012, ces documents – « the Global Intelligence Files »– seront publiés par WikiLeaks en collaboration avec plusieurs grands médias internationaux. Ces révélations feront état de nombreux abus de la

2. S'il existe des anecdotes faisant état de telles actions des les années 1980, il est selon Gabriella Coleman difficile d'établir l'existence de ces « hacks d'intérêt public » avant les années 2000 pour la simple raison qu'on ne dispose généralement pas d'informations précises sur la manière dont les documents publiés furent obtenus – le « hack » (si hack il y avait) n'étant pas revendiqué en tant que tel. Il s'agit là d'un terrain ouvert à des enquêtes historiennes (pour notre part nous avons trouvé au moins un exemple plus ancien que ceux qu'elle mentionne : un hack du groupe Virtual Monkeywrench, visant le forum de Davos en 2000, ayant permis de faire fuiter dans la presse suisse les noms de certains participants).

part de Stratfor : paiement de sources diplomatiques à l'aide de comptes off-shore, surveillance de groupes activistes pour le compte de grandes multinationales, gestion d'un fonds d'investissement sur la base d'informations secrètes récoltées par l'entreprise, entre autres. En 2013 et 2014, le hacker Phineas Phisher réussit à exfiltrer de nombreux documents internes à deux entreprises spécialisées dans la vente de vulnérabilités et de technologie de surveillance aux services de police et de renseignement : Gamma et Hacking Team.

Avec ces vols de données, une nouvelle génération de hackers reprend à son compte l'exfiltration de documents et permet de radicaliser la démarche de WikiLeaks, en contournant les lanceurs d'alerte, mais en augmentant aussi le risque juridique associé aux fuites (Heemsbergen, 2014). Grâce à eux, et avant même les révélations du lanceur d'alerte Edward Snowden sur les pratiques de surveillance de la NSA et des agences de renseignement alliées, les formes de la surveillance à l'ère numérique commençaient à nouveau à faire débat, et le rôle de petits acteurs privés dans ces assemblages était mieux documenté.

d. Construire l'autonomie médiatique des militants

À partir des années 1980, la minorité politiquement active de la mouvance hacker va tenter de faire vivre le projet d'une informatique émancipatrice en expérimentant ses usages contestataires, puis en participant avec l'arrivée d'Internet et du Web à une véritable « renaissance » du médiactivisme.

La péninsule italienne joue à cet égard un rôle important. En Italie, l'appropriation politique des réseaux informatiques dans les mouvements contre-culturels se produit à la croisée des milieux autonomistes, des travailleurs sociaux et des militants écologistes, et de mouvements artistiques inspirés par les arts de rue et le punk (Bazzichelli, 2009), notamment grâce à l'arrivée au sein de cette mouvance de FidoNet, un réseau fondé en 1984 qui permet de fédérer les BBS. Première plateforme de collaboration horizontale entre différentes communautés possédant leur propre infrastructure, il est vite adopté par des groupes militants en Amérique du Nord, en Europe, mais également en Afrique. Indépendant du gouvernement américain, – à l'époque, on surnomme encore le protocole TCP/IP le « DoD Protocol » pour « Department of Defence », afin de souligner sa filiation militaire et le décrédibiliser –, il fonctionne sur de petites machines, à l'aide de logiciels légers, et donc bien adapté à des environnements où l'accès aux ressources énergétiques et informatiques est limité.

En Italie, les premiers nœuds FidoNet apparaissent dès 1986 et constituent la base d'un réseau de groupes politiques et artistiques issus de différentes villes italiennes, auquel les participants apportent plusieurs innovations techniques pour répondre à leurs besoins. En 1989, sur la base d'un projet initialement porté par TV Stop, un groupe médiactiviste danois, FidoNet permettra le lancement du European Counter Network, qui réunit les franges radicales des mouvements sociaux européens et s'enracine durablement dans la péninsule italienne (maxigas, 2012 ; Milan, 2013). Ces expériences fondatrices conduisent à la multiplication de réseaux distincts, pour se concentrer sur des domaines spécifiques, comme l'opposition à la guerre, la défense des droits des immigrés, des collaborations artistiques, certains nœuds agissant comme des passerelles permettant de passer de l'un à l'autre.

Cette appropriation d'Internet par des groupes militants est largement permise par l'implication d'informaticiens engagés et autres hackers auprès d'organisations du mouvement social. Stefania Milan parle ainsi des années 1990 comme d'une période de renaissance pour le médiactivisme, avec l'arrivée d'une nouvelle génération de militants. Formés à l'informatique en réseaux lors de ses premières utilisations militantes dans les années 1980, ils vont chercher à mettre la puissance de ce nouvel outil aux mains des groupes militants, à « contourner les formes de fermeture et de contrôle actées par les États et les grandes entreprises », en œuvrant à « la création d'espaces

autonomes de communication » (Milan, 2013). Comptes e-mails, plateformes d'auto-publication, serveurs de messagerie instantanée et autres services d'hébergement mais encore les techniques d'anonymisation ou de collaboration font partie de la panoplie d'outils censés garantir l'autonomie communicationnelle des mouvements sociaux à l'ère numérique (Cardon et Granjon, 2010).

L'informatique en réseau permet alors d'approfondir les logiques réticulaires de résistance (Wolfson, 2014) : à l'ère de l'économie Fordiste, organisée dans le cadre de l'État-nation, les mouvements contestataires tendaient à épouser des modèles organisationnels centralisés et verticaux sur le modèle du « Parti ». À l'ère du capitalisme informationnel et de ses réseaux mondialisés, à l'ère de ce que Deleuze appelle la société de contrôle, les militants peuvent désormais construire grâce à Internet de multiples réseaux d'échanges et de solidarité articulant les échelles locales, nationales et mondiales.

Les hacklabs qui essaiment alors en Europe sont un lieu privilégié pour le développement de ces initiatives. Il s'agit d'espaces auto-gérés, le plus souvent situés dans des squats urbains, où des hackers organisent un accès libre à des ordinateurs (souvent des machines recyclées tournant sur GNU-Linux), des ateliers sur la programmation, sur la mise en place d'un site, d'une radio pirate, avec comme objectif d'offrir des outils et un savoir technique aux différents groupes militants qui gravitent autour de ces lieu (maxigas, 2012). De nombreux collectifs apparaissent alors : ACCII à Amsterdam ; Nodo 50 et SinDominio en Espagne ; Aktivix et PlentyFax au Royaume-Uni ; SO36 et Nadir en Allemagne ; Iventati en Italie, etc. Riseup.net, toujours en activité aujourd'hui, est sans doute le plus connu.

En France, le mouvement social de l'automne 1995 contre le projet de réforme des retraites catalyse ce genre d'expérimentations. Samizdat.net, formé en 1990, n'est alors encore qu'un petit groupe de trois ou quatre militants libertaires qui expérimentent avec un BBS et une mailing-list montée avec l'aide d'un projet anarchiste canadien du nom de Local Global (Papatheorodou, 2005). Ces expérimentations sont encore déconsidérées par les autres militants. Mais au cœur de la grève, alors que la plupart des canaux de communication (transports, postes) sont entravés, les syndicalistes de Sud se rendent compte de la puissance de ces outils, relativement aisés à l'usage et qui permettent de communiquer bien plus vite que les médias alternatifs traditionnels. Cet épisode fera l'effet d'un déclic, contribuant à réorienter l'activité de Samizdat, ainsi que l'expliquera plus tard l'un des cofondateurs du collectif, Aris Papatheorodou : « nous souhaitions offrir des outils pour que les gens engagés dans un mouvement soient capables d'eux-mêmes de transformer leurs actions en communication, et vice-versa, sans plus avoir besoin des médias traditionnels ou alternatifs ». Grâce à des amis italiens du European Counter Networks qui l'hébergent, Samizdat se met au Web dès janvier 1996. Quelques années plus tard, le groupe accueille près de 200 mailing-lists, offre de l'espace de stockage et son savoir-faire technique à divers groupes militants amis, et contribue à la mise en place de réseaux éphémères de collecte et de diffusion d'informations, notamment dans le cadre de contre-sommets altermondialistes.

En actant une désintermédiation sans précédant de l'espace public, en permettant aussi des formes d'anonymat, ces innovations socio-techniques défont une partie des mécanismes sur lesquels s'était fondé le droit de la communication (notamment, l'auto-régulation au sein des rédactions traditionnelles, sous l'égide du directeur de publication). Certains de ces intermédiaires techniques militants sont d'ailleurs victimes de répression (voir l'affaire Altern en France, ou le réseau Indymedia né en 1999 et associé à la mouvance altermondialiste, qui fera aussi l'objet de nombreuses perquisitions au début des années 2000). Dans cette mesure, on peut également intégrer ces stratégies à la panoplie des illégalismes hackers.

e. Contournement de la censure

En 1996, en pleine guerre de Yougoslavie, le fournisseur d'accès néerlandais pionnier de l'Internet militant XS4ALL, fondé par des hackers inspirés du CCC, va participer de la remise en celle d'un mode d'action expérimenté dès les années 1980 : le contournement de la censure. À Belgrade, la station de radio B92 constitue alors un des principal foyer d'opposition au gouvernement de Slobodan Miloševic (Markovic, 2000). À la propagande guerrière des nationalistes serbes, les journalistes B92 opposent une information indépendante promouvant la tolérance et le multiculturalisme en Yougoslavie qui détonne dans le paysage médiatique. Un positionnement qui conduit la police secrète serbe à tenter de les censurer, d'abord en brouillant leur fréquence. En 1996, XS4ALL aide alors la station à développer son propre réseau pour se connecter à Internet et diffuser ses bulletins d'information (bientôt relayés par Voice of Americas et BBC World}), mais également pour communiquer à travers des mails chiffrés.

Le réseau de B92, baptisé OpenNet, sert rapidement de point de ralliement à de nombreux sites et forums de discussion pour diverses ONG alors actives en Yougoslavie. C'est alors qu'interviennent plusieurs tentatives de la police secrète visant à intercepter le trafic entre OpenNet et XS4ALL. Début 1999, alors que le réseau académique yougoslave est encore le principal fournisseur d'accès à Internet, les proches de Miloševic au sein de l'enseignement supérieur décident unilatéralement de bloquer l'accès aux serveurs d'OpenNet. De nombreux hacktivistes leur viennent alors en aide pour mettre en place des sites miroirs (qui répliquent le site Internet sous un autre nom de domaine, et une autre adresse IP), dans le but de contourner cette tentative de blocage.

De même, lorsqu'en septembre 1996, un utilisateur du service d'hébergement d'XS4ALL décide de publier sur son site un exemplaire électronique de la revue de Radikal – un groupe allemand d'extrême gauche considéré comme terroriste en Allemagne et dont les écrits sont interdits –, le parquet allemand fait pression sur le réseau académique allemand, le Deutsches Forschungsnetz, qui accepte de bloquer l'accès aux serveurs. Six mille sites alors hébergés par XS4ALL sont censurés en Allemagne (Penenberg, 1997). De nouveau, des militants s'organisent et mettent en place une quarantaine de sites miroirs en place pour contourner le blocage.

Autre exemple : en 2001, le collectif Hacktivismo et le légendaire groupe de hackers Cult of the Dead Cow,– l'un des berceaux de l'hacktivisme fondé en 1984, alors engagé dans des actions d'aide aux dissidents chinois – publient un manifeste conjoint appelant au contournement de la censure (Ruffin, 2012). Prenant acte du développement des politiques de censure qui se développaient alors – notamment en Chine et dans les Pays du Golfe, avec le silence complice des régimes libéraux – le texte s'appuyait sur la Déclaration universelle des droits de l'Homme et sur le Pacte international relatif aux droits civils et politiques pour en appeler à la résistance :

> « Nous étudierons les moyens de contourner la censure étatique de l'Internet en mettant en œuvre des technologies pour défier les violations des droits de l'Homme. La censure étatique de l'Internet est une manifestation sérieuse de la violence organisée et systématique perpétrée contre les citoyens »

f. Censure temporaires (attaques en déni de service)

Dès le milieu des années 1990, des militants venus des communautés hackers vont aussi chercher à développer des formes originales de manifestation dans l'environnement numérique. En 1995, lorsque le président français Jacques Chirac décide la reprise des essais nucléaires français en Polynésie, un groupe d'activistes italiens œuvrant sous le nom du Strano Network, mené par le militant et artiste Tommaso Tozzi imagine une forme de protestation d'un nouveau genre dans le cadre d'une journée mondiale de mobilisation contre la décision des autorités françaises (Ludovico, 2005). Techniquement, l'action envisagée consiste à organiser une attaque distribuée en déni de service (*Distributed Denial of Service*, ou DDOS), qui consiste à rendre

indisponible un site Web en l'innondant de requêtes, contre certains services en ligne du gouvernement français : le but était de réunir un nombre conséquent de participants capables d'envoyer simultanément des requêtes vers le serveur cible, comme s'ils voulaient consulter les sites hébergés, au point de l'inonder, d'en ralentir le fonctionnement et de rendre les sites temporairement inaccessibles. Recrutés par le biais de mailing lists, de réseaux de BBS, mais aussi par la radio et les journaux militants, les participants à cette première « netstrike », -- c'est ainsi qu'est baptisé l'événement -- agissent de concert le 14 décembre 1995, entre 18h00 et 19h00, heure française (plutôt qu'une grève, il s'agit davantage de « la version en réseau d'un sit-in pacifique »).

Le procédé va faire école. Quelques mois plus tard, le Critical Art Ensemble (CAE) -- un groupe au croisement des arts performatifs et du militantisme -- théorise cette pratique pour l'inscrire dans l'éventail plus large des actions de « désobéissance civile électronique », dans un essai publié en 1996 (Critical Art Ensemble, 1996). Ce collectif transatlantique y appelle alors à une évolution des actions désobéissantes qui tiennent compte des mutations des systèmes de pouvoir. Le changement d'ère se caractérisant par le passage de l'univers physique vers le cyberespace, il faut selon eux que les formes de résistance migrent à leur tour dans l'environnement numérique et soient systématisées.

Des dissensions stratégiques vont toutefois survenir au sein du groupe, ce qui conduit à une scission et à la création en 1997 d'un autre collectif, l'Electronic Disturbance Theatre (EDT). Alors que ce dernier assume pleinement l'aspect symbolique de ces pratiques, les inscrivant dans le cadre de campagnes médias à la manière du Strano Network, les militants du Critical Art Ensemble se posent en puristes. Ils estiment pour leur part qu'il est illusoire de vouloir vaincre la bataille de l'opinion au travers des médias traditionnels, et préfèrent à l'intervention dans l'espace public la logique de la confrontation, de l'action directe clandestine, dans le but de saboter les architectures techniques des adversaires avec l'aide de hackers politisés.

Ces collectifs hacktivistes théoriciens de la « désobéissance civile électronique » s'inscrivent à leur tour dans le mouvement altermondialiste. L'un des premiers faits d'armes de l'EDT consiste ainsi à organiser un DDoS en solidarité avec la rébellion zappatiste, et visant notamment le site de la présidence mexicaine. En 1999, lors du sommet de l'OMC en 1999, la méthode et les outils de l'EDT développés pour organiser des DDoS politiques, sont repris par un groupe se faisant appeler les « electrohippies ». Une attaque DDoS est alors organisée contre plusieurs des sites de la conférence de Seattle dans le but de contrer la « propagande » en faveur des multinationales. Pour mener à bien cette opération de DDOS politique, le groupe propose aux manifestants de télécharger un outil Javascript développé par l'EDT. Ils revendiqueront près de 450 000 participants à ce sit-ins virtuel, mais l'action ne provoqua que quelques ralentissements sporadiques pour les sites visés.

Les electrohippies changeront ensuite de stratégie, organisant deux jours durant une campagne de mail-bombing, invitant les participants à envoyer des messages électroniques contenant des pièces jointes volumineuses afin d'inonder les serveurs mails des organisateurs de la conférence et entraver les communications internes (parmi les documents proposés pour les pièces jointes figuraient le protocole de Kyoto et des rapports émanant d'agences de protection de l'environnement). En 2001, deux organisations européennes vont également lancer des actions DDoS contre le site de la compagnie aérienne Lufthansa à laquelle participeront près de 13 000 personnes, dans le cadre d'une campagne visant à dénoncer la collaboration de l'entreprise dans l'expulsion des immigrés clandestins en Allemagne (Klang et Madison, 2016).

i) Défiguration de sites Web

La défiguration de site (*defacement*) fait également partie des formes de sabotage propres au répertoire d'action hacktiviste : les contrôles d'accès à l'interface d'administration du site Web visé sont alors déjoués au pour afficher en page d'accueil un message en forme d'avertissement ou de placard.

La mouvance Anonymous l'a pratiqué a plusieurs reprises à des fins d'expression politiques, par exemple en janvier 2014 pour le premier anniversaire du suicide d'Aaron Swartz, un militant des libertés sur Internet qui s'est donné la mort en janvier 2013. Pendant une heure, des membres du collectif ont réussi a diffuser en page d'accueil du site du MIT, critiqué pour avoir joué un rôle actif dans les poursuites pénales intentées contre le jeune activiste qui cherchait à « libérer » l'ensemble des archives académiques de JSTOR. Le message appelait les visiteurs du site à se joindre à une journée de manifestation en ligne – *The Day We Fight Back* –, organisée le mois suivant par l'EFF et son réseau internationale d'ONG partenaires pour dénoncer la surveillance de masse (Blue, 2014).

En 2012, Anonymous s'était également illustré par une action de défiguration massive de près de 500 sites liés au gouvernement chinois. Cette fois, les messages affichés indiquaient aux internautes chinois quelques outils pour se protéger contre la surveillance et de la censure, en les encourageant à organiser des manifestations contre le régime.

Conclusion : Les illégalismes hackers face au durcissement répressif

Ce rapide parcours dans quelques uns des épisodes paradigmatiques de la cristallisation du répertoire d'action rattachable au monde hacker, même pris dans son versant le plus militant et radical, mérite d'être approfondi. Mais il suffit à montrer la diversité des pratiques et des motivations qui s'y font jour.

Il y a d'abord une pluralité de rapports à l'informatique. Il existe en effet un réel écart dans l'appréhension des enjeux politiques associés aux ordinateurs et aux réseaux numériques entre des groupe technocritiques radicaux comme le CLODO ou les participants à *Processed World*, et les efforts de ceux qui travaillent à l'autonomie des mouvements sociaux. Dans un cas, il y a la conviction que ces nouvelles machines ne feront que renforcer l'asymétrie des rapports de force politique en devenant « un outil de plus » au service des dominants (la thèse du CLODO), tandis que de l'autre, on estime que l'ère numérique augure d'une « ère post-média » (Guattari, 1990) qui permettra de rompre les inégalités dans la capacité à intervenir politiquement et médiatiquement. Et au milieu, il y a ceux qui pensent encore qu'il est possible d'agir pour empêcher le renforcement de l'informatique technocratique et tentent de déceler ses vulnérabilités et ses lignes de fuites, et dont les fondateurs du CCC ou Julian Assange offrent des illustrations.

Au sein des partisans d'un même mode d'action, les avis divergent également sur les stratégies adéquates. Contre le Strano Network qui proposait d'inscrire les DDOS dans des campagnes médiatiques visant à nuire à l'image et à la réputation de multinationales ou d'organisations internationales, les hacktivistes de l'EDT l'imaginent comme un mode de sabotage relevant de l'action directe, visant à entraver le fonctionnement des organisations visées. En 2012, alors que des militants agissant sous la bannière d'Anonymous tentaient de censurer temporairement des sites à travers des attaques DDOS, un pionnier de l'hacktivisme et membre historique du groupe Cult of the Dead Cow avait d'ailleurs violemment critiqué leurs actions, estimant qu'on ne pouvait défendre la liberté d'expression en censurant ses adversaires (Ruffin, 2012).

Ce débat renvoie en réalité à des luttes classiques autour des frontières de la légitimité du sabotage, et plus largement à la question désobéissance civile, traditionnellement définie comme une action pacifique et non-violente. Or, la frontière entre mode d'action violent et non-violent

s'est largement déplacé ces trente dernières années. Au début des années 1980, les actions du CLODO avaient beau s'inscrire dans une période marquée par les débuts de l'antiterrorisme visant notamment l'extrême gauche, elles résonnaient néanmoins avec des craintes encore largement partagées dans la société quant aux conséquences et aux risques de l'informatisation. La bienveillance des policiers comme des médias à leur égard est tout-à-fait saisissante, alors même que leurs actes incendiaires engagent des dommages matériels conséquents. Un commissaire estime alors dans la presse qu'« il n'y a pas grand chose à faire » et, qu'en l'absence de personne blessées, « c'est aux boîtes elles-mêmes de se payer des gardiens » pour se prémunir de ce que la police qualifie alors « d'actions non violentes » (Izoard, 2010). Toujours dans la presse, un journaliste de *La Dépêche* reconnaît au CLODO le mérite d'« interpeller l'opinion », de « lui faire comprendre qu'une société entièrement livrée aux ordinateurs [peut] prêter le flanc aux pires répressions ». À *Libération*, le groupe est présenté comme un collectif « d'empêcheurs de programmer en rond », ses actes incendiaires qualifiés d'« actions symboliques ».

Dans les années qui suivent, les illégalismes de la mouvance hacker provoquent toutefois une véritable panique morale qui conduit déjà à l'adoption de législations pénales pour réprimer la « fraude informatique », et qui se traduit par des opérations de police spectaculaires (Sterling, 1993 ; Manion et Goodrum, 2000). Au tournant des années 2000, les États adaptent leurs législations pour s'assurer de la possibilité de poursuivre les actions hacktivistes (DDOS, hacks d'intérêt public) sur la base des dispositifs antiterroristes. Dans le même temps, on l'a évoqué, des sites participatifs associés à l'altermondialisme sont victimes de raids et de censures. La répression reprend de plus belles après 2010 : lorsque des hacktivistes décident de lancer des actions de DDOS contre Paypal pour dénoncer le blocus bancaire dont est victime WikiLeaks suite au Cablegate, Christopher Weatherhead, un étudiant alors âgé de 22 ans, est condamné en janvier 2013 par un tribunal de Londres à 18 mois de prison ferme. Il lui est reproché d'avoir administré le salon de discussion ayant permis l'organisation d'une de ces attaques de déni de service (Streams, 2012). Deux autres britanniques ayant joué un rôle encore plus secondaire sont condamnés à six et sept mois de prison ferme, et son réputés avoir agi en « bande organisée » (Viswanatha, 2014). Aux États-Unis, le jeune activiste Jeremy Hammond, déclaré coupable de la fuite des e-mails de Strafor, est condamné à dix ans de prison ferme en novembre 2013. En France, les DDOS conduits ces dernières années, par exemple au sein de collectifs écologistes, font l'objet d'un traitement policier et judiciaire complètement disproportionné, mobilisant les services de renseignement intérieurs et des techniques d'enquête spéciales (Tréguer, 2015). Les infiltrations, le recrutement d'informateurs, voire des formes de censure extralégales conduites par les services de renseignement contre des groupes de hacker politiques ont également été recensées (Coleman, 2014 ; Pilkington, 2014).

La disqualification des illégalismes propres à la mouvance hacker s'inscrit dans un contexte plus large, caractérisé par « l'inflation d'un moralisme anti-violence nourri par le discrédit de tout ce qui, du domaine des conduites individuelles comme des pratiques politiques, relève de la violence » (Girard, 2010). En retour, ce traitement répressif pousse ces modes d'action vers la clandestinité, invitant à remettre en cause les conceptions traditionnelles de la désobéissance civile qui, à l'image des théories de John Rawls ou de Hugo Bedau insistent sur l'idée que, pour que l'action désobéissante puisse être légitime, le militant doit être prêt à payer le prix de son illégalisme et donc accepter de se faire condamner pour avoir enfreint la loi (Hayes et Ollitrault, 2012)[3].

3. Selon ces conceptions « moralistes » de la désobéissance civile, l'acceptation du jugement peut aussi servir les fins stratégiques du désobéissant au travers de la mise en scène médiatique du procès ou même de l'emprisonnement, qui donne alors à voir la violence de la répression judiciaire face au citoyen désobéissant et pacifique convaincu de la justesse de sa cause.

Historiquement, certains groupes hackers ont voulu s'inscrire dans ces doctrines moralistes : Même s'ils invitaient les participants à protéger leur anonymat – par exemple en utilisant une adresse anonyme pour participer à des campagnes de *mail bombing* –, et même s'ils avertissaient ces derniers des risques juridiques qu'impliquaient les actions de piratage politique, les groupes hacktivistes pionniers comme les electrohippies n'hésitaient pas à révéler l'identité des organisateurs de ces actions et revendiquaient de ne pas recourir au chiffrement des communications. Le fait de s'identifier constituait selon eux une garantie de la légitimité et du caractère responsable de leur protestation. Après tout, au travers de ces actions qu'ils concevaient comme le prolongement numérique des manifestations de rue, ils ne faisaient qu'exercer un droit constitutionnellement garanti. Le fait que les autorités puissent chercher à encadrer l'exercice de ce droit leur semblait dès lors faire partie des règles du jeu établies de longues date dans l'espace physique (par exemple, la déclaration préalable d'une manifestation). Même si la réponse des autorités à cette nouvelle forme d'activisme demeurait incertaine, même si le spectre de l'antiterrorisme était une menace réelle, il leur semblait que cette réponse resterait proportionnée, qu'ils seraient considérés comme des militants et non comme des criminels et encore moins comme des terroristes. De ce point de vue, il leur était possible d'écrire dans uns de leurs manifestes : « *We have nothing to hide* » (electrohippies collective, 2000).

Or, comme le remarque Molly Sauter (2014), dans les pratiques contemporaines du piratage hacktiviste, et en particulier au sein de la mouvance Anonymous, l'anonymat a clairement pris le dessus. Comme son nom l'indique, l'anonymat a toujours constitué un ciment culturel d'Anonymous, et ce bien avant que la mouvance ne se politise (et c'est évidemment un trait fort de la culture hacker, les electrohippies apparaissant plutôt comme une exception de ce point de vue). En outre, à l'image d'autres groupes subversifs et autrement plus offensifs comme les Black Blocs, Anonymous utilise la dissimulation pour créer un effet politique : son icône (le masque de Guy Fawkes) de même que son slogan (« *We are Anonymous. We are legion (...)* ») participent en effet d'une marque politique évoquant une horde évasive et insoumise, cherchant par là-même à construire une puissance symbolique inversement symétrique à celle de l'État centralisé et surplombant, tout en marquant le rejet des écueils de la représentation interne au mouvement. Enfin et surtout, l'environnement politique s'est lui-même transformé. Si les premières communautés hacktivistes pouvaient prendre pour modèle les figures les plus classiques de la désobéissance civile et de la manifestation de rue, les dernières générations du mouvement opèrent près de quinze ans plus tard dans un contexte répressif nettement plus tendu.

De fait, depuis la période post-Cablegate marquée par les coups d'éclat de la mouvance Anonymous, la répression de l'hacktivisme réengagée à partir de 2011 semble avoir porté ses fruits, en ce sens que nombre des modes d'action présentés ici semblent délaissés. Même en faisant abstraction des risques associés à la répression, l'économie politique de l'informatique s'est transformée : les illégalismes hackers sont apparus dans un contexte où quelques militants isolés mais compétents et motivés pouvaient encore tenir en échec les infrastructures de puissantes organisations. L'évolution du marché de la cybersécurité et de l'informatique elle-même – avec une concentration croissante de la ressource en calcul – rend a priori moins plausible le fait qu'un conflit asymétrique tourne à l'avantage des hackers politiques. La concentration du Web militant au sein des grandes plateformes réduit également les marges de manœuvre des militants et les exposent aux nouveaux assemblages public-privé dédiés à la surveillance et à la censure (Klang et Madison, 2016 ; Tréguer, 2019b). Quant aux sabotages physiques expérimentés par le CLODO, ils se heurteraient sans doute non seulement aux législations anti-terroristes, mais aussi au fait que les data centers sont devenue de véritables forteresses (Carnino et Marquet, 2018). L'espace juridico-politique et les possibilités socio-techniques qui, historiquement, sous-tendaient les illégalismes hackers semblent bien être aujourd'hui réduites à portion congrue.

Bibliographie

Assange J. *State and Terrorist Conspiracies*. *Arch. IQorg*. 10 novembre 2006.

Bazzichelli T. *Networking: The Net as Artwork*. BoD – Books on Demand, 2009.

Blondeau O. *Devenir média: l'activisme sur Internet, entre défection et expérimentation*. Paris : Amsterdam, 2007.

Blue V. « MIT website hacked by Anonymous on anniversary of Aaron Swartz suicide ». *ZDNet*. 2014.

Bowcott O., Hamilton S. *Beating the System: Hackers, Phreakers and Electronic Spies*. London : Bloomsbury Publishing PLC, 1990. 224 p.

Cardon D., Granjon F. *Médiactivistes*. Paris : Les Presses de Sciences Po, 2010.

Carlsson C. (éd.). *Bad Attitude: The Processed World Anthology*. London ; New York : Verso, 1990. 282 p.

Carnino G., Marquet C. « Les datacenters enfoncent le cloud : enjeux politiques et impacts environnementaux d'internet ». *Zilsel*. 13 février 2018. n°3, p. 19-62.

Coleman G. « Hacker ». Ryan M-L, Emerson L, Robertson BJ (éd.). *Johns Hopkins Guide Digit. Media*. Baltimore : John Hopkins University Press, 2014a. p. 245-249.

Coleman G. « Phreaks, Hacker, and Trolls: The Politics of Transgression and Spectacle ». *Soc. Media Read.*. New York University Press, 2012.

Coleman G. « The Public Interest Hack ». *Limn*. juin 2017. n°8 Disponible sur : < http://limn.it/the-political-meaning-of-hacktivism/ >

Coleman G. « The Latest Snowden Revelation Is Dangerous for Anonymous — And for All of Us ». *WIRED*. 2014b. Disponible sur : < http://www.wired.com/2014/02/comes-around-goes-around-latest-snowden-revelation-isnt-just-dangerous-anonymous-us/ >

Costanza-Chock S. « Mapping the Repertoire of Electronic Contention ». Opel A, Pompper D (éd.). *Represent. Resist. Media Civ. Disobedience Glob. Justice Mov.* Westport, Conn. : Praeger, 2003. p. 173-191.

Critical Art Ensemble. *Electronic civil disobedience and other unpopular ideas*. Autonomedia & Critical Art Ensemble, 1996.

Deleuze G. « Post-scriptum sur les sociétés de contrôle ». *Autre J.* 1990. n°1.

Denker K. « Heroes Yet Criminals of the German Computer Revolution ». Alberts G, Oldenziel R (éd.). *Hacking Eur. - Comput. Cult. Demoscenes*. Springer, 2014. p. 167-188.

DJNZ, Action tool development group of the electrohippies collective. « Client-side Distributed Denial-of-Service: Valid campaign tactic or terrorist act? ». *Electrohippies Occas. Pap.*. février 2000. n°1.

Dominguez R. « Electronic Civil Disobedience: Inventing the Future of Online Agitprop Theater ». *PMLA*. 1 octobre 2009. Vol. 124, n°5, p. 1806-1812.

Dreyfus S., Assange J. *Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier*. Edimbourg : Canongate Books, 2012.

Georgen A. « Il y a 30 ans, le Chaos Computer Club entrait dans la légende en hackant le minitel allemand ». *Slate.fr*. 2014. Disponible sur : < http://www.slate.fr/story/94973/ccc-legende-hacker-minitel-allemand >

Girard M. « Du dedans au dehors de l'espace démocratique : la désobéissance civile ». *Multitudes*. 2010. Vol. 41, n°2, p. 212.

Greenberg A. *This Machine Kills Secret: How Wikileakers, Hacktivists, and Cypherpunks are Freeing the World's Information*. Virgin Books, 2012. 384 p.

Gros F. « Foucault et « la société punitive » ». *Pouvoirs*. 1 novembre 2010. Vol. 135, n°4, p. 5-14.

Guattari F. « Vers une ère post-média ». *Terminal*. novembre 1990. n°51

Hayes G., Ollitrault S. *La désobéissance civile*. Paris : La Découverte, 2012. (Contester ; 10).

Heemsbergen L. J. « Designing hues of transparency and democracy after WikiLeaks: Vigilance to vigilantes and back again ». *New Media Soc.*. 24 février 2014.

Izoard C. « L'informatisation, entre mises à feu et résignation ». Biagini C, Carnino G (éd.). *Les Luddites En France. Résistances à l'industrialisation et à l'informatisation*. Montreuil : Editions L'échappée, 2010.

Jarrige F. *Technocritiques: Du refus des machines à la contestation des technosciences*. La Découverte, 2016. 384 p.

Jordan T. *Hacking: Digital Media and Technological Determinism*. John Wiley & Sons, 2013.

Jordan T., Taylor P. *Hacktivism and Cyberwars: Rebels with a Cause?* Routledge, 2004.

Klang M., Madison N. « The domestication of online activism ». *First Monday*. 10 juin 2016. Vol. 21, n°6.

Levy S. *Hackers: Heroes of the Computer Revolution*. Anv Upd. O'Reilly Media, 1984.

Levy S. *Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age*. 1st edition. London : Penguin Books, 2001.

Ludovico A. « »Loading Error …« - The first netstrike took place ten years ago ». *Springerin.at*. 2005.

Lunceford B. « Building Hacker Collective Identity One Text Phile at a Time: Reading Phrack ». *Media Hist. Monogr.*. 2009. Vol. 11, n°2.

Manion M., Goodrum A. « Terrorism or Civil Disobedience: Toward a Hacktivist Ethic ». *SIGCAS Comput. Soc.* juin 2000. Vol. 30, p. 14–19.

Markovic S. « Radio B92 and OpenNet - Internet Censorship Case Study ». *APC Eur. Internet Rights Proj.*. 2000.

Maxigas. « Hackers against technology: Critique and recuperation in technological cycles ». *Soc. Stud. Sci.*. 1 décembre 2017. Vol. 47, n°6, p. 841-860.

Maxigas. « Hacklabs and hackerspaces – tracing two genealogies ». *J. Peer Prod.*. juillet 2012. n°2. Disponible sur : < http://peerproduction.net/issues/issue-2/peer-reviewed-papers/hacklabs-and-hackerspaces/ >

Milan S. *Social Movements and Their Technologies: Wiring Social Change*. Palgrave Macmillan, 2013.

Myers West S. « Survival of the Cryptic ». *Limn*. février 2017. n°8 Disponible sur : < http://limn.it/survival-of-the-cryptic/ >

Papatheorodou A. « Samizdat.net, l'histoire d'un projet de médias alternatifs sur Internet. Entretien avec Aris Papatheorodou ». *Matériaux pour l'histoire de notre temps*. 2005. Vol. 79, n°1, p. 57-62.

Penenberg A. L. « German Academic Net Blocks Dutch Site ». *Wired*. 1997. Disponible sur : < http://archive.wired.com/politics/law/news/1997/04/3265 >

Pilkington E. « LulzSec hacker "Sabu" released after "extraordinary" FBI cooperation ». *The Guardian*. 27 mai 2014. Disponible sur : < http://www.theguardian.com/technology/2014/may/27/hacker-sabu-walks-free-sentenced-time-served >

Razac O. *Avec Foucault, après Foucault : Disséquer la société de contrôle*. Paris : Editions L'Harmattan, 2008.

Ruffin O. *Anonymous, India and the Blackhat Spectacle*. *Kafila*. 7 juin 2012. Disponible sur : < http://kafila.org/2012/06/07/anonymous-india-and-the-blackhat-spectacle-oxblood-ruffin/ >

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

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

Streams K. « Anonymous "Operation Payback" hackers convicted for costly DDoS attacks ». *The Verge*. 2012. Disponible sur : < http://www.theverge.com/2012/12/6/3735622/anonymous-conviction-christopher-weatherhead-operation-payback >

Tréguer F. *L'action directe contre l'informatisation (1960-1990)*. 14 juin 2019a. Disponible sur : < https://www.wethenet.eu/2019/06/laction-directe-contre-linformatisation/ >

Tréguer F. « Le droit pénal de la fraude informatique, nouvel ami des censeurs ? ». *Rev. Droits L'homme - Actual. Droits-Lib.*. 2 juin 2015. Disponible sur : < https://revdh.revues.org/1328 >

Tréguer F. « Vers l'automatisation de la censure politique ». *La Quadrature du Net*. 22 février 2019b. Disponible sur : < https://www.laquadrature.net/2019/02/22/vers-lautomatisation-de-la-censure-politique/ >

Viswanatha A. « "Anonymous" hackers plead guilty to minor charge in U.S. for cyberattacks ». *Reuters*. 19 août 2014. Disponible sur : < http://www.reuters.com/article/2014/08/19/us-anonymous-cybercrime-plea-idUSKBN0GJ25720140819 >

Wieckmann J. *Danger pirates informatiques*. Plon, 1989.

Wolfson T. *Digital Rebellion: The Birth of the Cyber Left*. 1st Edition edition. Urbana : University of Illinois Press, 2014.

Wright S. « Beyond a Bad Attitude? Information Workers and Their Prospects Through the Pages of Processed World ». *J. Inf. Ethics*. octobre 2011. Vol. 20, n°2.

« Névrosés de la programmation ». *Le Monde*. 18 avril 1989. Disponible sur : < http://www.lemonde.fr/archives/article/1989/04/18/nevroses-de-la-programmation_4112894_1819218.html >

Terrorism Review. CIA, 1983. (General CIA Records). Disponible sur : < https://www.cia.gov/library/readingroom/document/cia-rdp84-00893r000100130001-6 >