Détruire ou altérer le fonctionnement des machines numériques, la résistance du 21e siècle ?

Par **Benjamin Cadon**

Luddisme > néo-luddisme

Plus de deux siècles se sont désormais écoulés depuis la destruction de deux métiers à tisser par le légendaire Capitaine Ludd en 1780 en Angleterre. Leader imaginaire du mouvement luddite, Ned Ludd incarna la colère des tondeurs et tricoteurs anglais, premières victimes d'une paupérisation et d'un libéralisme économique naissant. Sentant leur mode de travail artisanal menacé par l'arrivée des métiers à tisser industriels, ils s'attachèrent à les détruire pour ne pas se voir dépossédés de leurs savoir-faire et de leurs conditions de vie. Ce mouvement connut des échos en France et dans d'autres pays, des groupes se sont ensuite opposés à l'arrivée du train (Jarrige 2010) ou à l'électrification.

Cette forme d'opposition radicale au « progrès technologique » a ressurgi avec le développement de l'industrie informatique dans les années 80 pour donner lieu au néo-luddisme. Entre 1978 et 1995 le mathématicien Theodore Kaczynski, alias « Unabomber », enverra des dizaines de colis piégés à des informaticiens et à des professeurs renommés de Yale ou Berkeley et tuera trois personnes et en blessera une vingtaine d'autres. Traumatisé par les expériences de résistance au conditionnement psychologique conduites à Harvard, irrité contre les mouvements de femmes et de noirs, il quitte le monde universitaire en 1969 pour fomenter ses attentats et devenir le plus célèbre terroriste anti-technologie de l'histoire. Les textes qu'il a diffusés ont connu un certain écho et sont aujourd'hui encore réédités. Ils exposent néanmoins des motivations parfois douteuses sous-tendues par une critique des technologies qui reste sommaire (Giffard 2017).

En contrepoint, on peut évoquer le toujours mystérieux « Comité pour la liquidation ou le détournement des ordinateurs (Clodo) » (Izoard 2010) qui a sévi à Toulouse entre 1980 et 1983 et a réalisé des « sabotages d'artistes » en incendiant des ordinateurs et des supports de stockage dans des entreprises du numérique jusqu'au centre informatique de la préfecture. Composé de « travailleurs informatiques », ils s'attaquaient à travers l'ordinateur à « l'outil préféré des dominants », qui sert « à exploiter, à ficher, à contrôler et à réprimer », qui contribue à « renforcer la domination idéologique et économique de l'Occident et spécialement des États-Unis et, à un moindre degré, celle des pouvoirs locaux » (CLODO 1983, 5) à l'échelle mondiale.

40 ans plus tard, le « numérique » s'est incrusté jusque dans nos intimités, pour autant les technocritiques

d'un terreau fertile pour l'éclosion de collectifs technocritiques comme « Pièces et Mains d'Œuvre » ou « Technologos », de maisons d'édition comme La lenteur ou L'échappée. D'autre part, les écrits du Comité invisible (« Fuck Google ») ou d'auteurs comme Bernard Stiegler ou Eric Sadin connaissent une plus grande diffusion sans pour autant galvaniser les masses laborieuses. Cependant, ces dernières années, nous avons assisté à une recrudescence d'actes de sabotages d'objets technologiques à la fois pour des motivations technopolitiques et aussi pour des raisons nourries de désinformation.

Pourquoi autant de haine à l'égard de ces chères machines ?

On ne peut que constater le succès écrasant du capitalisme numérique vis à vis d'utopies révolutionnaires et libertaires désormais déchues (Tréguer 2020). Le numérique, un temps fantasmé comme facteur de partage de connaissances et d'ouverture à la diversité, facteur de liberté d'expression vis à vis de médias monopoligarchiques. Ce numérique a finalement donné naissance à Qanon, monstre né des réseaux sociaux après s'être échappé d'un canular parti en Larsen, bête multimédiatique apte à électriser l'attention autour d'un président des États-Unis symbole de toutes les dérives de l'espèce humaine. Le numérique comme facteur constitutif de la réalité, comme moteur de la « gouvernementalité algorithmique » (Rouvroy et Berns 2013), comme agent de surveillance ubiquitaire, entre crainte, fascination et désarroi. On aurait déjà atteint le « Point de singularité technologique » en ayant créé des technologies dont la complexité nous échapperait au profit d'intelligences artificielles qui prendraient subtilement le gouvernail de nos destinées. Ce mille-feuilles technologique dans lequel on s'empêtre, si complexe et efficace soit-il, parfois dysfonctionne et s'attire alors toutes les foudres humaines.

Les technologies échappent à notre entendement, à l'image de la sulfureuse « 5G », certes déployée sans l'assentiment des populations, sans études sanitaires indépendantes (Bérard 2020), à grand renfort d'arguments éculés (« un plus gros débit », « la médecine connecté »). Cette « 5G » a cristallisé un agglomérat invraisemblable de vrais et de fausses informations conduisant des individus et groupes à brûler des antennes de téléphonie parfois pas encore « 5G ». Cette haine renaissante à l'égard des machines se nourrit donc à la fois d'une pensée technocritique qui s'élabore, mais aussi de matière mentale parasitée par les réseaux sociaux. Face à cette perte d'emprise, des initiatives valeureuses fleurissent pour se réapproprier ces technologies et tenter de préserver nos libertés dans un combat dissymétrique.

Le logiciel libre s'est fait encloser par le capitalisme

Le projet GNU/Linux et la licence GPL de Richard Stallman ont constitué de valeureuses tentatives pour contrecarrer l'accaparement de richesses intellectuelles et économiques de l'informatique par des logiques propriétaires de copyright. Ces logiques furent promues par de grandes entreprises qui avaient bien compris que la rente se déplaçait du matériel au logiciel, avant de tomber dans la donnée. Cette tentative valeureuse fut rapidement dépassée par la droite par le mouvement de l'Open Source pour lequel les valeurs éthiques importaient peu, tant que cela marchait mieux et que l'on pouvait embarquer votre code libre dans les codes que l'on garde fermés.

Par sa malice, Microsoft a réussi à conserver sa mainmise sur le système d'exploitation des ordinateurs, Google a réussi son *hold-up* sur les mobiles avec Android (système ouvert quand cela l'arrange), les logiciels libres quant à eux sont majoritairement utilisés pour faire fonctionner Internet (Wikipédia 2021) et ses multiples protocoles, même Microsoft se met à Linux pour son *cloud* (Fassinou 2020). Et si l'on regarde quels sont les plus gros contributeurs aux standards d'Internet (Ten Oever 2021) ou au développement du noyau Linux, on retrouve les géants du numérique en tête : Intel, Google, Huawei, Facebook, AMD, NVIDIA, IBM, CISCO, et bien d'autres géants … qui forgent leur propre intérêt. Car ces licences et logiciels libres restent dans une vision libérale du régime de la propriété et s'emprisonnent dans le capitalisme, à l'inverse de l'approche « copyfarleft » de Dimitry Kleiner. Les multinationales du numérique s'en accommodent donc très bien, pendant que de petits chatons (voir https://chatons.org/), en tentant de *dégoogliser* Internet, usent leurs griffes en vain. Internet a beau être mu par des logiciels libres, ce n'est pas le sentiment de liberté qui y prévaut aujourd'hui. Car fondamentalement, comme Julia Laïnae et Nicolas Alep le signalent, on peut considérer que « Le logiciel libre n'est qu'une modalité de développement informatique et de licence de diffusion, il ne remet pas en cause la recherche d'efficacité, la rationalité instrumentale, qui sont au fondement des technologies numériques » (Laïnae & Alep 2020). Face à cette dystopie technologique, que fait le politique ?!

Des rapports non-consentis avec les technologies

Les technologies qui nous sont « proposées » aujourd'hui sont rarement le fruit d'un choix collectif « démocratique » qui aurait statué, à l'issue d'un débat informé sur le bien-fondé, d'implanter la technologie en question dans nos quotidiens. Depuis l'invention des relations publiques par Edward Berneys, les agences de marketing ont grandement peaufiné leurs recettes pour susciter chez nous un désir irrépressible d'acquérir les dernières innovations technologiques comme gage d'appartenance et d'adhésion à un futur technologique présenté comme inéluctable. Ce futur a su remporter l'adhésion d'une majorité de personnalités politiques en constituant le levier d'une croissance économique potentiellement infinie car supposément immatérielle, la « croissance verte grâce au numérique » devient une évidence. Toute critique du système techno-capitaliste en place se voit ainsi qualifiée de rétrograde, de conspiration à pulls longs visant à nous renvoyer chez les amish (Kelly 2009) éclairés à la bougie. Günther Anders (1956) lui-même considérait qu'il était impossible de critiquer la technique « sans se condamner à une mort intellectuelle, sociale ou médiatique » (p. 17).

Cette perte d'emprise sur nos modes de vie et d'interactions sociales de plus en plus médiés par des technologies conduit à un sentiment d'impuissance face à cette technostructure opaque. Des usages et des détournements tactiques de ces technologies numériques de l'information et de la communication ont permis des formes de résistance, cette dernière décennie a aussi vu la montée en puissance de postures plus radicales visant à briser les machines et les réseaux, je vous propose ici d'en réaliser en inventaire partiel et partial.

Un inventaire néo-luddite

Péter les plombs

Privés d'électricité, un ordinateur (serveur) marche beaucoup moins bien, il peut être alimenté temporairement par un onduleur ou secouru par des groupes électrogènes s'il est hébergé dans un *datacenter*. Les antennes de téléphonie mobiles ne disposent que de quelques heures d'autonomie la plupart du temps sans alimentation électrique.

À l'échelle locale, provoquer un court-circuit dans un réseau électrique s'avère fort simple et efficace car les interfaces avec le réseau, les prises électriques, pullulent en intérieur comme en extérieur, mais l'impact reste limité car chaque branche est protégée par un disjoncteur.

À distance, le virus Stuxnet, un ver informatique découvert en 2010, a pu s'attaquer aux centrifugeuses iraniennes d'enrichissement d'uranium et provoquer leur autodestruction sans alerter les opérateurs sur place. Ce ver apprécie particulièrement les systèmes industriels SCADA, des automates programmables industriels produits par Siemens et utilisés dans les centrales hydro-électriques ou nucléaires, destinés à la distribution d'eau potable, les oléoducs ou la gestion de la circulation des trains. Il a très certainement été conçu par une alliance de la NSA avec l'unité israélienne 8200, mais on est donc là plutôt dans le registre de la cyberguerre. En mars 2018, le Département de la Sécurité intérieure américain (Department of Homeland Security ou DHS) révélait que la Russie pénétrait régulièrement son réseau d'énergie depuis 2017. On la soupçonne également d'avoir provoqué deux *black-out* en Ukraine en 2015 et 2016, avec deux virus, Black Energy et Industroyer, qui ont plongé 230 000 résidents dans le noir pendant une à six heures (Sautreuil et Deprez 2017). En Allemagne fin 2014, des pirates informatiques prenaient le contrôle d'un haut-fourneau allemand et détruisaient une partie des infrastructures lourdes. En 2016, la centrale nucléaire de Gundremmingen, située à 120 kilomètres au nord-ouest de Munich, a été visée par plusieurs attaques informatiques d'ampleur.

Le 16 avril 2013, une attaque sophistiquée a été menée contre la sous-station de transmission Metcalf de la *Pacific Gas and Electric Company* à Coyote, en Californie, près de la frontière de San Jose. L'attaque, au cours de laquelle des hommes armés ont tiré sur 17 transformateurs électriques, a entraîné des dommages matériels d'une valeur de plus de 15 millions de dollars et a miraculeusement eu peu d'impact sur l'alimentation en électricité de la région mais restera comme « the most significant incident of domestic terrorism involving the grid that has ever occurred » (Wikipédia 2020). Plus récemment, une petite compagnie d'électricité américaine a recruté elle-même des hackers afin de tester la fiabilité de son système de sécurité. Seulement trois jours ont suffi aux pirates pour entrer physiquement dans les bâtiments de la compagnie, puis dans la totalité du réseau, en dérobant au passage les données privées de 50 000 clients, pour finir par provoquer une coupure de courant (Demeure 2016).

Dans cette charmante ambiance, difficile de distinguer les motivations des protagonistes, aujourd'hui plus téléguidés par des États et des velléités belliqueuses que par une envie romantique de détruire la société techno-industrielle en la vidant de son jus.

Couper les câbles

En septembre 2009, plus de 500 salariés d'Alcatel ont creusé le sable de la plage de Beg-Léguer à Lannion (Côtes-d'Armor), afin de déterrer le câble transatlantique Apollo, qui relie les États-Unis à l'Europe. L'objectif était de faire apparaître le câble, mais pas de le couper. « Aucune dégradation n'est envisagée », avaient prévenu les syndicats qui inventent ici un mode de lutte inédit (Ouest-France 2009).

En mars 2016, Hayastan Shakarian, retraitée géorgienne, aurait sectionné un câble d'un coup de pelle pour revendre le métal, mettant ainsi en panne plusieurs heures une bonne partie des réseaux Internet de l'Arménie, de la Géorgie et de l'Azerbaïdjan. La « hackeuse à la pelle » n'avait jamais entendu parler d'Internet.

Depuis, de multiples actes de vandalisme ont été constatés sur des fibres optiques aux États-Unis, notamment sur des lignes dédiées au *trading* à haute fréquence. De même, en France on assiste à une multiplication des actes de sabotage, une proposition de loi visant à lutter contre les actes de vandalisme commis sur les réseaux de fibre optique en France a été déposée en juin 2020 (Reda 2020).

L'infrastructure du réseau a en effet de nombreux points de fragilité, le récent incendie d'un data center OVH à Strasbourg a démontré le nombre de sites et services contenu dans petit parallélépipède parti en fumé. Fort heureusement, les multinationales du numérique investissent massivement pour avoir leurs propres tuyaux transocéaniques, pour bien sur consolider le réseau de façon altruiste, neutre et décentralisée.

Brûler les antennes

La destruction de l'antenne de Roc'h Trédudonen en Bretagne en 1974 priva la population de cette région du service télévision pendant 3 mois, « les Bretons redécouvrent la vie de leurs grands-parents, les librairies font recette et les veillées nocturnes reprennent » (Wikipédia 2020b). Le Front de Libération de la Bretagne ne sévit plus, de multiples flux de télévision atteignent désormais cette région française, bientôt véhiculés par la 5G.

Plus récemment, partout dans le monde, des personnes et des groupes se sont mis à brûler ou à détruire des antennes de téléphonie mobile. À l'origine, un amalgame pétri par les réseaux sociaux suscite une partie de ces velléités destructrices, selon lequel Bill Gates aurait anticipé, voire prémédité, la crise du Covid pour implanter des vaccins-puces connectés en 5G à l'ensemble de la population mondiale. Il est vrai que la connaissance des effets sur la santé du déploiement massif de la 5G pose

question. Il est vrai que la fondation dirigée par Bill Gates est devenue le premier financeur de l'OMS (Laurentdhomme 2020). Il est vrai que l'on connaît très peu les effets à long terme de l'inoculation de ces vaccins innovants. Le déploiement de la 5G implique l'installation d'antennes de longue portée et de proximité, ajoutant une couche indigeste à hautes fréquences au brouillard électromagnétique déjà bien garni sans même les 40 000 satellites du projet Starlink d'Elon Musk.

Détruire les excroissances

On a vu ces dernières années de multiples projets de jeune pousse (*start-up*) coloniser l'espace public avec une diversité de trottinettes et d'autres vélos connectés en libre-service. Leur destruction de la manière la plus spectaculaire possible est devenue, dans certains pays, un jeu sur les réseaux sociaux : lancées depuis le toit d'un immeuble, autodafées sur la place publique, tentatives de transformer ces objets en sous-marins ou avions par catapultage. De façon plus légère, des plaisantins hackers ont aussi modifié des trottinettes Lime pour leur faire diffuser des messages inappropriés (Dozier 2019).

Mouvement mondial de lutte contre cette forme d'écophagie technologique ou simple plaisir vandale ? Dans certains pays, ces entreprises ont prétexté que ces comportements destructeurs, ce manque de « civisme », mettaient à mal leur modèle économique et ont décidé de cesser leurs activités, laissant à la collectivité publique le soin de débarrasser et traiter ces objets connectés devenus déchets. Parfois, des entreprises comme Uber détruisent 20 000 vélos électriques neufs parce que les actionnaires ont changé de braquet (Peters 2020).

Dans ce registre de destruction des excroissances de la société technologique, on pourrait également évoquer celle des radars automatiques en France perpétrée par des personnes impliquées dans le mouvement des « Gilets jaunes » : sur 4500 appareils, 600 ont été mis hors service dont plus de 130 détruits par les flammes en 2018 provoquant une chute de recettes pour l'état.

Tuer les ordinateurs

Le « USB killer » a été prototypé en 2015 puis proposé à la vente car potentiellement correspondait à un marché : branché sur n'importe quel port USB, il se charge très rapidement et envoit une forte tension à la carte mère auquel il est relié, provoquant très souvent le décès irrévocable de la machine incriminée ou, à minima, la mort du contrôleur USB. Des youtubeurs se sont emparés de l'objet pour le tester sur de multiples marques d'ordinateurs, de téléphones, mais aussi sur des distributeurs de boissons, des consoles de jeu, voire des voitures. Cette orgie de furie destructrice non conscientisée est ambiguë (Usb Killer 2017) : les démonstrateurs sont souvent surpris de l'effet de leur acte tout en étant souvent sponsorisés par les marques d'appareils qu'ils détruisent. « Youtube sans conscience, … . »

Dénier le service

Dans l'attirail du néo-luddite, le déni de service (distributed denial-of-service – DDoS) est un outil prisé. Il consiste à saturer un serveur avec des requêtes répétées et tordues afin qu'il tombe en carafe. Il implique de pouvoir produire un grand nombre de requêtes idéalement issues d'une grande diversité d'origines pour surpasser les capacités de réponse et de filtration du serveur. Le groupe informel « Anonymous » a usé à de multiples reprises cette technique pour provoquer le dysfonctionnement de serveurs d'entreprises ou d'administrations ciblées. Gabriella Coleman a analysé la politisation de ce mouvement protéiformes (Coleman 2015), finalement troublée par la compromission de Sabu, l'une des figures du mouvement « Anonymous », avec la CIA, rendant son implication dans le mouvement « Occupy wall street » trouble.

Le déni de service est, la plupart du temps, non-destructif, il est aussi souvent utilisé pour maltraiter ses concurrents, notamment dans le *dark Web*. Il a été popularisé via les « Anonymous » et des outils faciles d'accès comme LOIC (Wikipédia 2021) qui ont engendré des formes d'implications politiques par des biais numériques de personnes habituellement en marge du schéma « citoyen » traditionnel.

Offusquer les données

Si l'on considère la donnée comme le nouveau pétrole, on peut chercher à brouiller les pistes en utilisant des réseaux comme Tor ou en chiffrant ses messages via PGP. De façon plus simple et malicieuse, le *plug-in* de navigateur web AdNauseam va cliquer pour nous de façon hiératique sur de multiples publicités pour brouiller notre profilage marketing. Des chercheurs ont montré qu'avec des bouts de Scotch, on pouvait tromper une intelligence artificielle (Ackerman 2017). Se fondre dans la masse ou chiffrer ses données pour augmenter le coût de la surveillance et se rendre illisible constituent des stratégies complémentaires qu'il faut manipuler avec habileté au regard de la grandeur des oreilles qui écoutent.

De façon plus brutale, les rançongiciels qui chiffrent les données d'un ordinateur en le rendant inutilisable se sont répandus de façon exponentielle ces dernières années. De multiples services publics et entreprises furent touchés, parfois en renvoyant les salariés au papier-crayon pour pouvoir assurer un minimum d'activités. À priori, les motivations premières pour diffuser ce genre de virus sont financières, le versement d'une certaine somme d'argent en Bitcoin sur le compte indiqué étant susceptible de donner la clef d'accès aux précieuses données, mais il s'avère que ces transactions financières peuvent être suivies assez précisément (Paquet-Clouston, Haslhofer et Dupont 2019). Bizarrement, certains de ces virus maître-chanteur étaient conçus pour ne pas récupérer l'argent ni fournir la clef libératrice aux ordinateurs paralysés.

Altérer le fonctionnement

Il existe de multiples tactiques pour se prémunir de la surveillance numérique, qui peuvent passer par la destruction de caméras de surveillance ou l'utilisation de parapluies. Parfois une alliance inter-espèce non déclarée provoque l'atterrissage de drones de la police suite à l'intervention d'un couple de cormorans irrité par l'appareil et harangué par la foule des manifestants parisiens.

Dans la Silicon Valley, plusieurs mouvements de protestation se sont érigés contre les grandes entreprises du numérique coupables, entre autres, d'utiliser les voies réservées aux transports en commun avec leurs bus privés, et de gentrifier la région en rendant le logement inaccessible aux classes populaires. Des bus convoyés par Yahoo ! et Google à San Francisco furent bloqués, des manifestations furent organisées à la sortie de ces entreprises, des salariés ont été harcelés en ligne et jusqu'à leur domicile.

Les stratégies de destruction pour mettre un grain de sable dans ce capitalisme numérique galopant sont multiples et contextuelles : incendie de la Casemate, un FabLab à Grenoble, lutte contre l'implantation de Google à Berlin ou d'Amazon à New-York, destruction partielle d'une usine de production d'iPhone en Inde pour protester contre le non-versement des salaires (Amadeo 2020) et les conditions de travail, piratage militant du réseau inter-bancaire SWIFT pour saper la confiance (Fisher 2019), et bien d'autres stratégies.

Conclusion

Néo-luddisme > Low-tech

Indéniablement, le néo-luddisme revêt une force d'interpellation revitalisante face à des populations scotchées à leur écran et perfusées par les discours techno-solutionnistes. Les motivations de ces personnes et collectifs sont pour autant très disparates et contextuelles, myriade de formes de protestations contre un monde dont on aurait perdu les clefs au profit d'un système machinique perfide.

Aussi radicales et protéiformes qu'elles soient ces formes de critique de la technologie, elles contribuent à politiser la question technique, à déconstruire sa pseudo neutralité, à ramener dans l'agora les algorithmes et robots qui nous entourent. D'un point de vue environnemental, détruire des technologies complexes et difficiles à recycler n'est pas optimal au niveau entropique. Au regard des ressources naturelles existantes, on pourrait se demander si nous ne sommes pas allés trop loin trop vite dans le développement technologique. L'obsolescence recherchée des appareils et applications conduit à une impasse écologique, on pourrait plutôt rechercher l'invention, la production, l'échange, la maintenance de « technologies pour la vie », respectueuses de leur environnement, appropriées au contexte sociotechnique de la situation.

Là où la cyberculture défendait la création de zones autonomes temporaires, les mouvements zadistes et technocritiques se rejoignent plutôt sur l'idée de créer des zones autonomes durables. Pour François Jarrige (2010), la force du mouvement des Zones à défendre (Zad) vient de sa capacité à combiner « les trois grands champs de la technocritique telle qu'elle a pu s'exprimer depuis trois siècles, à savoir la critique morale fondée sur la quête d'autonomie, la critique sociale pourfendant l'inégalité, et la critique écologique, qui voit dans le gigantisme technicien une cause de la dégradation de la Terre ».

Faut-il rentrer allègrement dans l'âge des *low tech*, en s'orientant résolument « au plus vite et à marche forcée vers une société essentiellement basée sur des basses technologies, sans doute plus rudes et basiques, peut-être un peu moins performantes, mais nettement plus économes en ressources et maîtrisables localement »?, se demande Philipee Bihouix (2014).

Biographie

Benjamin Cadon est artiste et coordinateur de la Labomedia-mediahackerfablabspace, une association à but non lucratif basée à Orléans (France). Pour en savoir plus : https://labomedia.org

Références

Ackerman, Evan. 2017. « Slight Street Sign Modifications Can Completely Fool Machine Learning Algorithms ». En ligne : IEEE Spectrum, https://spectrum.ieee.org/cars-that-think/transportation/sensors/slight-street-sign-modifications-can-fool-machine-learning-algorithms (Page consultée le 4 août 2017)

Amadeo, Ron. 2020. « iPhone factory workers say they haven't been paid, cause millions in damages ». En ligne : Ars Technica. https://arstechnica.com/gadgets/2020/12/worker-protests-at-indian-iphone-factory-causes-up-to-7-million-in-damages/ (Page consultée le 15 décembre 2020)

Anders, Günther. 1956. L'obsolescence de l'homme : Sur l'âme à l'époque de la deuxième révolution industrielle. Paris : Éditions Ivrea.

Bérard, Nicolas. 2020. 5g mon amour : Enquête sur la face cachée des réseaux mobiles. Le Passager Clandestin.

Bihouix, Philippe. 2014. L'Âge des low tech. Vers une civilisation techniquement soutenable. Paris : Le Seuil.

CLODO. 1983. « Le CLODO parle... ». En ligne : Terminal 16. http://www.revue-terminal.org/magazine/archives/terminalN16.zip

Coleman, Gabriella. 2015. Anonymous – Hacker, activiste, faussaire, mouchard, lanceur d'alerte. Montréal : Éditions Lux.

Demeure, Yohan. 2016. « Ils piratent un réseau électrique en 3 jours seulement ! ». En ligne : SciencePost. https://sciencepost.fr/piratent-reseau-electrique-3-jours/ (Page consultée le 21 juin 2016)

Dozier, Rob. 2019. « Des trottinettes hackées font des blagues déplacées en Australie ». En ligne : Vice. https://www.vice.com/fr/article/mb8epb/des-trottinettes-hackees-font-des-blagues-deplacees-en-australie (Page consultée le 4 mars 2019)

Fassinou, Bill. 2020. « Linux est le système d'exploitation le plus utilisé dans Microsoft Azure ». En ligne : Développez.com. https://windows-azure.developpez.com/actu/303007/Linux-est-le-systeme-d-exploitation-le-plus-utilise-dans-Microsoft-Azure-plus-de-50-pourcent-des-coeurs-de-machine-virtuelle-tournent-sous-Linux/

Fisher, Phineas. 2019. « HackBack – A DIY Guide To Rob Banks ». En ligne : Hackback. https://packetstormsecurity.com/files/155392/hackback-bankrobbing.txt

Giffard, Alain. 2017. « Kaczynski ». En ligne : Blog d'Alain Giffard. https://alaingiffardblog.wordpress.com/2017/12/15/kaczynski/ (Page consultée le 15 décembre 2020)

Izoard, Célia. 2010. « L'informatisation, entre mises à feu et résignation », dans : C. Biagini et G. Carnino (Dir.), Les Luddites en France, pp. 251-286. Le Kremlin-Bicêtre : Les Éditions L'échappée.

Jarrige, François. 2010. « Refuser de se laisser ferrer », dans : C. Biagini et G. Carnino (Dir.), Les Luddites en France, pp. 175-210. Le Kremlin-Bicêtre : Les Éditions L'échappée.

Kelly, Kevin. 2009. « Amish Hackers ». En ligne : The Technium. https://kk.org/thetechnium/amish-hackers-a/ (Page consultée le 10 février 2019)

Kleiner, Dmytri. 2010. The Telekommunist Manifesto. Network Notebooks 03. Amsterdam: Institute of Network Cultures.

Laïnae, Julia et Nicolas Alep. 2020. Contre l'alternumérisme. Saint-Michel-de-Vax : Éditions La Lenteur.

Laurentdhomme. 2020. « OMS ET FONDATION BILL GATES, CE QUE LE COVID REVELE ». En ligne : Mediapart. https://blogs.mediapart.fr/laurentdhomme/blog/100520/oms-et-fondation-bill-gates-ce-que-le-covid-revele (Page consultée le 10 mai 2020)

Lundi Matin. 2018. « ÉTATS-UNIS : UNE MYSTÉRIEUSE VAGUE DE VANDALISME CONTRE LES TROTTINETTES EN LIBRE-SERVICE. » En ligne : Lundi Matin. https://lundi.am/Etats-Unis-une-mysterieuse-vague-de-vandalisme-contre-les-trottinettes-en-libre (Page consultée le 19 septembre 2020)

Mao, Blaise. 2016. « Les ennemis de la machine ». En ligne : Usbek et Rica. https://usbeketrica.com/fr/article/les-ennemis-de-la-machine (Page consultée le 5 août 2016)

Ouest-France. 2009. « Les ennemis de la machine ». En ligne : Ouest France. https://www.ouest-france.fr/bretagne/lannion-22300/lannion-les-salaries-dalcatel-ont-deterre-une-partie-du-cable-transatlantique-562855 (Page consultée le 17 septembre 2020)

Paquet-Clouston, Masarah, Bernhard Haslhofer et Benoît Dupont. 2019. « Ransomware payments in the Bitcoin ecosystem », Journal of Cybersecurity 5 (1): 1-11.

Peters, Adele. 2020. « Uber just destroyed thousands of electric bikes ». En ligne : Fast company. https://www.fastcompany.com/90510167/uber-just-trashed-thousands-of-electric-bikes (Page consultée le 27 avril 2020)

Rouvroy, Antoinette et Thomas Berns. 2013. « Gouvernementalité algorithmique et perspectives d'émancipation, Le disparate comme condition d'individuation par la relation ? », Réseaux 1 (177): 163-196.

Reda, Robin. 2020. Proposition de loi visant à lutter contre les actes de vandalisme commis sur les réseaux de fibre optique. France : assemblée nationale. https://www.assemblee-nationale.fr/dyn/15/dossiers/alt/lutte_actes_vandalisme_reseaux_fibre_optique

Revue Terminal. 1983. Interview du CLODO. En ligne : Revue Terminal. http://www.revue-terminal.org/magazine/archives/terminalN16.zip

Sautreuil, Pierre et Fabrice Deprez. 2017. « Ukraine, anatomie d'une cyberguerre – épisode 1 : la menace au quotidien ». En ligne : Numerama. https://www.numerama.com/politique/283573-en-ukraine-la-cyberguerre-au-quotidien-episode-1-la-menace-permanente.html (Page consultée le 5 septembre 2017)

ten Oever, Niels. 2021. « 'This Is Not How We Imagined It': Technological Affordances, Economic Drivers, and the Internet Architecture Imaginary. », New Media & Society 23 (2): 344–62.

Tréguer, Félix. 2020. L'utopie déchue. Paris : Fayard.

Usb Killer. « usb killer compilation YouTube. » Vidéo YouTube, 13:53. https://www.youtube.com/watch?v=X4OmkBYB4HY (Page consultée le 30 janvier 2017)

Wikipédia, l'encyclopédie libre. « Serveurs publics sur Internet. », dernière modification le 3 avril 2021. https://fr.qaz.wiki/wiki/Usage_share_of_operating_systems#Public_servers_on_the_Internet

Wikipédia, l'encyclopédie libre. « Low Orbit Ion Cannon. », dernière modification le 11 janvier 2021. https://fr.wikipedia.org/wiki/Low_Orbit_Ion_Cannon

Wikipédia, l'encyclopédie libre. « Metcalf sniper attack. », dernière modification le 20 octobre 2020. https://en.m.wikipedia.org/wiki/Metcalf_sniper_attack

Wikipédia, l'encyclopédie libre. « Attentat de Roc'h Trédudon. », dernière modification le 2 septembre 2020. https://fr.wikipedia.org/wiki/Attentat_de_Roc%27h_Tr%C3%A9dudon