Les ruses du hacktivisme, aux frontières de l'engagement politique : retour sur Anonymous

Benjamin Loveluck

Quaderni n° 103, 2021, p. 71-88

Les ruses du *hacktivisme*, aux frontières de l'engagement politique : retour sur Anonymous

Benjamin Loveluck

i3-SES, Télécom Paris

Le mouvement Anonymous, principalement actif pendant la période 2008-2013, est l'auteur de multiples actions directes numériques telles que le blocage ou le détournement provisoire de sites web d'institutions ou d'entreprises, l'intrusion dans des systèmes d'information, la divulgation ou la publicisation d'informations confidentielles ou personnelles, et dans certains cas le harcèlement d'organisations ou d'individus ciblés. Ces actions revendiquent un caractère collectif et combinent le plus souvent une dimension spectaculaire et une forte visibilité médiatique avec des modalités d'intervention et d'organisation visant à dissimuler l'identité de leurs auteurs : elles relèvent ainsi d'une forme d'action clandestine numérique, mettant en œuvre une articulation particulière du secret et de la publicité.

Les Anonymous furent l'objet d'une remarquable fascination médiatique (Klein, 2015). On a peut-être oublié aujourd'hui à la fois le degré d'attention qu'ils ont suscité, et les craintes autant que les espoirs parfois disproportionnés qu'il ont pu soulever. Après les attentats perpétrés à Paris en 2015, leur « déclaration de guerre contre Daesh » fut relayée et applaudie (sans être suivie d'effets très probants). À l'inverse en 2012, le directeur de la NSA déclarait (de manière peu convaincante) que le groupe pouvait constituer une menace pour la sécurité nationale des États-Unis ; en réaction, un éminent juriste et spécialiste d'internet prenait leur défense en les qualifiant d'« *idée, de* zeitgeist » dont le moteur serait l'irrévérence, mais aussi de « *mouvement de contestation* » dont les actions seraient avant tout symboliques (Benkler 2012). Les « défacements » de sites web s'apparenteraient ainsi à des graffitis numériques et les blocages à des *sit-in* virtuels, destinés à exprimer un message temporaire au sein de l'espace numérique, et relèveraient selon le point de vue du vandalisme ou de l'expression politique. Cependant une succession de fuites de données confidentielles, dont certaines ont permis de dévoiler de graves abus de la part d'entreprises privées de renseignement, a finalement entraîné l'intervention du FBI et l'arrestation de certains membres, parfois condamnés à de lourdes peines de prison[1]. D'autres types d'actions se situent dans une zone plus trouble car ciblant directement des personnes : par exemple les initiatives visant à dénoncer nommément des individus suspectés de viol ou encore des membres présumés du Ku Klux Klan.

Les motifs et revendications des Anonymous, lorsqu'ils sont invoqués, vont de la défense de la liberté d'expression à la lutte contre les injustices et abus de pouvoir divers (corruption, pédopornographie), mais dans de nombreux cas les justifications sont plus floues voire inexistantes et il est difficile d'établir une « cause commune » identifiable. Dans la mesure où il s'agit de mobiliser des moyens informatiques pour intervenir dans l'espace public, les Anonymous ont été qualifiés de « hackers activistes » ou *hacktivists*, ce qui suppose une forme d'action politique militante (Jordan 2001 ; Jordan & Taylor 2004). Mais ils se présentent également sous les traits de justiciers masqués émanant de la « *multitude* » des internautes (Hardt et Negri, 2000) et agissant de manière distribuée à

des fins punitives. De manière générale, les cadres d'analyse établis par la sociologie des mouvements sociaux et de l'action collective rendent difficilement compte d'une identité collective aussi labile et d'une telle diversité de finalités (McDonald 2015 ; Uitermark 2017).

L'anthropologue Gabriella Coleman a publié en 2014 un ouvrage sur le mouvement, dont elle a suivi certains des épisodes les plus marquants. Traduit en français en 2016, ce livre tient lieu aujourd'hui de référence sur Anonymous, aussi bien sur le plan méthodologique à travers l'ethnographie en ligne d'un mouvement difficile à circonscrire, que par le récit haletant et détaillé qu'elle dresse de sa trajectoire. Analysant quelques années plus tard l'héritage du mouvement, elle estime qu'Anonymous engage des actions de « *désobéissance, de défiance et de contestation* » qui consistent à concentrer l'attention médiatique sur un enjeu donné et à « *porter un jugement – souvent expéditif – sur les actions d'individus, d'organisations ou de gouvernements* » ; pour arriver à leurs fins ils « *exploitent un aspect de notre condition numérique collective* », c'est-à-dire la vaste collection de données réalisée par les entreprises et les autorités, à laquelle ils accèdent (légalement ou non) et qu'ils font fuiter afin de générer de la publicité et ternir la réputation de leurs cibles (Coleman 2020, p. 160-161, notre traduction). Le caractère spectaculaire est accentué par l'anonymat et l'imprévisibilité du mouvement, qui produit du suspense et des effets de surprise.

Coleman pointe certaines ambiguïtés – une part d'irresponsabilité, des actions justicières mal avisées, des factions telles que LulzSec[2] dont la justification politique est mince – mais trace au final le récit d'une prise de conscience politique. Dans la conclusion de son ouvrage (2016), elle insiste sur le « *militantisme politique solide* » du mouvement. Ses ambivalences l'apparentent selon elle au *trickster*, le « décepteur » qui peuple les mythes et légendes, mais pour avoir simplement montré que « *la disruption et le changement* » sont possibles, il se présente pour Coleman avant tout comme un esprit de résistance voire un « *principe espérance* », en référence aux initiatives, symboles et artefacts qui incarnent l'espoir à travers l'histoire, rassemblés par le philosophe Ernst Bloch (1885-1977). Des questions importantes demeurent cependant, s'agissant de la véritable nature politique du mouvement – dont le bien-fondé des actions est finalement tributaire des vertus morales que l'on peut (ou non) leur assigner. L'enjeu de sa représentativité est également occulté derrière la rhétorique de la multitude (« Nous sommes Anonymous. Nous sommes légion »).

L'objet de cet article est de questionner ces ambivalences en revenant sur les modes de coordination et d'action des Anonymous, à partir de travaux existants ainsi qu'une observation participante menée en janvier 2015 (lors d'une éphémère « réactivation » du mouvement à l'occasion des attentats à Paris). Si l'histoire du mouvement a déjà été documentée, le recul dont nous disposons aujourd'hui permet en effet d'évaluer à nouveaux frais la portée de ses activités. Les pratiques auxquelles les Anonymous ont recours – la simulation et la dissimulation, la surprise et l'opportunisme, le détournement mais aussi l'audace – manifestent à la fois une forme d'intelligence créatrice et une tromperie délétère, qui renvoient au caractère équivoque de la ruse. Detienne et Vernant dans leur travail sur l'intelligence rusée ou *mètis* des grecs relèvent ainsi ses « *traits essentiels* » : « *souplesse et polymorphie, duplicité et équivoque, inversion et retournement, [qui] impliquent certaines valeurs attribuées au courbe, au souple, au tortueux, à l'oblique et à l'ambigu, par opposition au droit, au direct, au rigide et à l'univoque* » (1974, p. 55). Ce sont ces caractéristiques qui permettent de prendre l'ascendant dans un contexte de pouvoir asymétrique, qui demande de se tenir caché mais aux aguets, de tendre des pièges et de saisir des occasions, de changer de forme et de jouer avec le masque des apparences (*ibid*., p. 19-31). Or à l'aune de cette catégorie, nous montrons que si Anonymous manifeste un véritable brio tactique, sa signification politique peine à émerger : la ruse apparaît en effet souvent comme une fin en soi, *un mode d'action en quête d'une cause* bien plutôt que l'inverse, qui verse fréquemment dans des formes de justice sommaire. D'une certaine manière, la *mètis* des Anonymous semble ainsi se laisser enfermer dans sa propre « *circularité* ».

Nous rappelons tout d'abord que si le mouvement a pu agréger à certains moments de nombreux participants venus d'horizons différents, son noyau dur s'est constitué en des lieux bien précis – le site 4chan et des messageries IRC – où se sont également établis des codes d'interaction communs ainsi qu'une dynamique de groupe : c'est à partir de cette « base arrière » d'initiés que des actions collectives clandestines ont pu être mises en œuvre. Nous nous intéressons ensuite à l'inflexion qu'a connue le mouvement à partir de 2008, qui en élargissant son champ d'action et en construisant une image

médiatique de hackers justiciers et masqués émanant du « peuple » d'internet, a été amené à apporter des justifications d'ordre politique à ses actions : c'est donc à l'épreuve de l'espace public et en cherchant à capter l'attention collective que les Anonymous ont endossé le rôle de « hacktivistes ». Nous détaillons enfin pour terminer certaines des tactiques déployées, et notamment les *ruses de la visibilité* qui lui permettent de générer des effets spectaculaires. En conclusion, si l'habileté tactique du mouvement lui a permis d'accumuler des coups d'éclats et de poser un certain nombre de problèmes publics, elle interroge également les frontières de l'engagement politique à l'ère numérique.

Se reconnaître et s'organiser entre initiés

Anonymous est né au début des années 2000 sur le forum 4chan, initialement dédié au partage d'images de mangas et d'anime japonais (*imageboard*). Faiblement modéré, cet espace revendiquait par le biais de son fondateur (Christopher Poole, alias « moot ») une totale liberté d'expression. Celui-ci défendait les vertus de l'anonymat des utilisateurs sur le site et le caractère « *brut, non filtré* » de leurs contributions, en contrepoint à l'extension des réseaux sociaux tels que Facebook et plus généralement du contrôle sur l'identité et l'expression exercé par les plateformes numériques (Poole, 2010)[3].

4chan incarne toute l'« *ambivalence* » de l'internet contemporain (Phillips & Milner, 2017). Avec d'autres plateformes telles que Reddit, ce fut d'abord le lieu d'une parole libérée semblant échapper à la censure. Bien qu'ayant beaucoup évolué depuis ses débuts (le site est désormais plus contrôlé), pour ses défenseurs il fut l'un des hauts lieux de la culture vernaculaire numérique et l'un des principaux héritiers des premiers espaces de socialisation en ligne tels que les *newsgroups* et autres formes de *message boards* et de forums (Stryker, 2011). Le forum était marqué par la dérision, l'ironie et l'humour noir, ainsi qu'une inclination pour les canulars (*pranks*) – en particulier sur l'une des sections les plus populaires du site appelée /b/ ou « *random* ». Mais pour ses détracteurs, mettant l'accent sur les aspects les moins reluisants du site, c'est avant tout un espace de circulation de contenus scabreux (pornographiques notamment) et d'une parole débridée qui, sous couvert d'ironie et de transgression, donne libre cours à des propos homophobes, misogynes et racistes, et qui se présente également comme la matrice de nombreuses campagnes de harcèlement. Le site – et tout particulièrement la section /pol/ (« *politically incorrect* ») – a par ailleurs été identifié comme l'un des repaires de l'*alt-right*, ce mouvement d'extrême droite suprémaciste qui fut très actif pour promouvoir en ligne le candidat Donald Trump lors des élections présidentielles américaines de 2016 (Hine *et al.*, 2017 ; Nagle, 2017).

C'est pourtant au sein de cet espace que les membres de Anonymous ont constitué une première culture commune et des pratiques partagées. Par défaut, le site ne demande pas aux utilisateurs de s'enregistrer, et chaque contributeur se voit donc attribuer le même identifiant – « Anonymous » – rejoignant ainsi la « communauté » des « Anons ». Par ailleurs, le site présente un caractère éphémère car il n'archive pas les contenus : une contribution chasse l'autre et selon le degré d'activité de la section et des *threads* (fils de discussion), ces contributions sont accessibles plus ou moins longtemps (Bernstein, M.S. *et al.*, 2011). Paradoxalement, l'anonymat et la fugacité des interactions ont pour effet de renforcer les liens entre participants : ce n'est qu'après avoir pratiqué le forum un certain temps que les échanges prennent sens, et ce n'est qu'en demeurant actif que l'on accède à la mémoire collective et à la culture partagée du forum, qui évolue en permanence. En outre les modalités d'expression, le vocabulaire et le capital de références mobilisables contribuent à entretenir un certain degré d'ésotérisme et à former un entre-soi extrêmement codifié et exclusif (bien que très conflictuel), marquant une séparation d'avec les « *normies* » c'est-à-dire les personnes ordinaires et « conformistes », extérieures à 4chan ou qui n'en maîtrisent pas les subtilités (Nissenbaum et Shifman, 2017).

En parallèle, certains participants échangent sur des messageries instantanées ou *Internet Relay Chat* (IRC) qui, sous couvert de pseudonymes, autorisent les participants à discuter directement entre eux ou bien à rejoindre des canaux dédiés (*channels*), et permettent par exemple de coordonner des actions en lançant des mots d'ordre et en échangeant des informations. L'IRC fut très populaire pendant les années 1990 avant l'arrivée de services commerciaux dédiés, et permet de créer des espaces de communication dont les administrateurs gardent le contrôle, dans la mesure où ils gèrent leurs propres serveurs. Il constitue selon Guillaume Latzko-Toth (2008) « *un* monde *en soi, régi par des normes et ponctué de rituels* ». Les communications peuvent être sécurisées afin d'éviter que les contributeurs

soient identifiés, tout en étant ouvertes au plus grand nombre. Mais leur utilisation demande une certaine acculturation, l'interface étant assez austère. Il existe en outre différents niveaux de confidentialité, et si une partie des échanges est publique et facilement accessible, d'autres canaux sont « privés » voire « secrets » et d'accès plus restreint.

De manière générale, la volonté de participer aux activités des Anonymous nécessite de s'impliquer dans les échanges tenus sur ces messageries, les plus connues étant accessibles via des plateformes telles que AnonOps – « *ops* » renvoyant ici à « opérateurs IRC » qui jouent le rôle d'administrateurs, mais dénotant également l'idée d'« opérations » conduites par le mouvement[4]. Une sous-section du site appelée « OpNewBlood » est destinée aux nouvelles recrues. Quelques faits d'armes et vidéos des Anonymous sont mis en avant, mais le site propose surtout de leur fournir « *le masque, la cape et le chapeau* » à travers un ensemble de tutoriels sur l'utilisation de l'IRC et l'anonymisation des communications à travers des consignes de sécurité ainsi que des conseils techniques sur l'utilisation d'outils de chiffrement (illustration 1).

Illustration 1 : https://newblood.anonops.com, capture d'écran, 27 novembre 2015

Ces observations permettent d'éclairer les conditions préalables aux actions clandestines numériques des Anonymous, qui nécessitent aussi bien l'acquisition de compétences communicationnelles que l'établissement de liens de confiance entre les participants. Celle-ci se tisse d'abord à travers des codes culturels et une socialisation partagés qui permettent d'initier et d'enrôler les membres, et parallèlement par l'établissement graduel de liens plus étroits au sein d'espaces permettant un filtrage plus granulaire des niveaux d'engagement (et des risques afférents).

Du trolling *aux actions politiques :* hacker *l'espace public*

Au-delà de ses origines immédiates sur 4chan et des forums fréquentés par de jeunes *geeks*, Anonymous se nourrit de la culture et de l'imaginaire *hacker*. Bien que les trajectoires et l'éthique personnelle des *hackers* soient très hétérogènes, la maîtrise des outils techniques, mais aussi l'affirmation de l'autonomie individuelle face aux systèmes d'information et enfin une propension au *détournement ingénieux* constituent une matrice commune (voir l'avant-propos de ce numéro). Des *hackers* chevronnés se sont parfois joints aux actions du groupe pour des motivations diverses – par conviction politique mais aussi par défi, ou simplement pour jouer avec cette identité collective. Et le mouvement dans son ensemble s'appuie sur la mystique du *hacker* comme « sorcier » (*wizard*) capable d'assujettir les systèmes techniques à sa volonté et capable d'en retourner la logique à ses propres fins.

Cependant les actions déployées par les Anonymous ne demandent souvent pas de compétences numériques très poussées, mais sont plutôt orientées vers la communication (communiqués, montages, vidéos), la coordination entre les différents groupes, et dans certains cas la capacité à trouver des informations publiquement disponibles mais difficiles d'accès (Coleman 2020, p. 159). Bien que certaines failles techniques relativement accessibles soit exploitées, il s'agit avant tout de « *hacker l'économie de l'attention* » (boyd, 2010 ; Stryker, 2011) en manipulant l'information et en tirant profit des vulnérabilités de l'espace public, afin de renverser les rapports de pouvoir. L'inclination pour la discrétion voire la clandestinité souvent associée au *hacking* peut ainsi entrer en tension avec une « *politique de la transgression et du spectacle* » conduite par le groupe (Coleman 2012), en particulier lorsque les actions trouvent un retentissement dans des espaces médiatiques plus vastes.

Comme le souligne Coleman (2016), à l'origine les actions relevaient avant tout du *trolling* : des provocations destinées à perturber – voire *saboter* – le cours des choses, ce qui situe d'emblée cette démarche dans le registre de la ruse trompeuse. La finalité avancée était fréquemment : « *doing it for the lulz* », qui implique une forme d'humour cynique et souvent aux dépens d'un tiers, par contraste implicite avec le rire *mainstream* et naïf des masses (*lulz* est une déformation de LOL, *laughing out loud*). Ces actions prennent la forme de pièges ou d'offensives dont les formes varient : elles vont du canular téléphonique (un grand classique) à la diffusion d'informations personnelles, et dans certains cas donnent lieu à des assauts collectifs qualifiés de « raids » ciblant des jeux en ligne (notoirement le jeu Habbo Hotel en 2006) mais aussi des organisations ou des personnes. Cette pratique est elle-même liée à la culture des jeux multi-joueurs en ligne (voir Golub, 2010).

Malgré des apparences potaches, le *trolling* peut rester cantonné à une forme de jouissance de son propre pouvoir et n'est pas non plus une pratique anodine (Phillips 2015). Outre les discours et contenus outranciers en circulation, lorsqu'il est dirigé contre des individus ciblés il relève parfois purement et simplement du harcèlement ou de l'humiliation – souvent à caractère sexiste, raciste ou homophobe. Selon Coleman cependant, un point de bascule est intervenu en 2008, lorsque des Anonymous se sont « politisés » en entreprenant de coordonner une action contre l'Église de Scientologie – c'est-à-dire en dirigeant cette fois leurs efforts contre une organisation. Appelé « Project Chanology » (en référence à 4chan), il s'agissait de s'attaquer au « double maléfique » des Anonymous (Coleman, 2016, Ch. 2). L'une des bêtes noires des défenseurs de la liberté d'expression, la Scientologie a depuis longtemps déployé des moyens juridiques considérables pour intimider ses détracteurs sur internet (en s'appuyant souvent sur des prétextes de propriété intellectuelle) – et fait elle-même figure d'organisation secrète, à caractère sectaire. Elle souhaitait cette fois-ci censurer une vidéo de promotion interne de l'organisation mettant en scène l'acteur Tom Cruise, qui avait fuitée. Une panoplie de méthodes bien rodées furent utilisées, allant des canulars téléphoniques aux commandes multiples de pizzas ou de taxis, en passant par l'envoi d'images pornographiques ou le blocage de fax par l'envoi de pages noires (*black fax*), et enfin la perturbation des sites web de l'organisation par des connexions massives – attaque dite par « déni de service » ou DDoS (*distributed denial of service*) qui consiste à « faire tomber » un site (le plus souvent pour un bref moment) en multipliant massivement les connexions vers ce site.

À la différence des précédents exploits du groupe, la dynamique persista plusieurs semaines, et se mua en un mode d'intervention nouveau. Une vidéo en forme de « déclaration de guerre » fut diffusée, qui consistait en une succession de plans fixes sur des immeubles et des nuages, accompagné d'une voix robotique lisant un communiqué se terminant par ce qui allait devenir la signature du

mouvement : « *We are Anonymous. We are legion. We do not forgive. We do not forget. Expect us* »[5]. Par la suite et pour la première fois, des manifestations physiques récurrentes ainsi que différents *happenings* de nature carnavalesque furent organisés dans des dizaines de villes à travers le monde. De nombreux Anonymous se rencontrèrent ainsi hors ligne, permettant dans certains cas de renforcer le sentiment d'appartenance. Des consignes furent également publiées à cette occasion – l'une d'entre elles encourageant les participants à couvrir leur visage pour éviter d'être identifiés. C'est ainsi que beaucoup de manifestants décidèrent de recourir au fameux masque de Guy Fawkes tiré du roman graphique *V for Vendetta* (Moore et Lloyd, 1988-89)[6], dont certaines représentations étaient déjà en circulation sur 4chan.

Ce masque grimaçant est devenu l'emblème et la principale ruse des Anonymous, dont il capture plusieurs dimensions clés. Il signale en effet d'une part la dissimulation de l'identité individuelle des membres, d'un point de vue tactique afin d'échapper à la surveillance et aux potentielles conséquences juridiques de leurs actions, et ainsi provoquer la surprise. D'autre part, il constitue également un signe de ralliement et participe à la construction d'une identité collective distribuée, destinée à asseoir la légitimité de ces actions, censées émaner de la « multitude ». Enfin, il ajoute une dimension théâtrale dans la mesure où les Anonymous entretiennent l'idée d'une volonté abstraite, mystérieuse et capable de frapper à tout moment : un « esprit de l'internet » qui viendrait punir ceux qui le défient ou qui enfreindraient le code moral dont ils sont dépositaires.

Le large écho médiatique donné à ces événements contribua à en amplifier la portée et la signification. Dans le même temps, la dimension de croisade morale nouvellement acquise fut contestée par une partie des membres, comme étant antagoniste aux pratiques et aux « valeurs » (ou l'absence de valeurs) en vigueur sur 4chan, certains dénonçant les velléités des « défenseurs de la justice sociale » (SJW ou *social justice warriors*). Ces divergences de vue entraînèrent de nombreuses dissensions, qui ont continué de traverser le mouvement, jusqu'à donner naissance à des sous-groupes voire des factions rivales telles que LulzSec, AntiSec ou Lizard Squad, animées avant tout par l'esprit de provocation originel et réalisant souvent des exploits techniques plus poussés[7]. Mais pour tous les acteurs concernés, le surcroît de publicité modifia sensiblement la nature des actions entreprises, qui se déroulaient désormais devant un public beaucoup plus vaste et en fonction de logiques médiatiques différentes.

Après 2008, de nombreuses actions furent lancées (au moins une centaine, la période 2011-2012 étant la plus active)[8], d'ampleur variable et dirigées contre des cibles très diverses. La plus importante d'entre elles, qui propulsa véritablement le mouvement sur le devant de la scène médiatique, fut déclenchée à la fin de l'année 2010. Appelée « Operation Payback », et basculant cette fois plus nettement du côté de l'illégalité, elle était initialement menée contre des entreprises de l'industrie du divertissement, des associations interprofessionnelles défendant la propriété intellectuelle, ainsi que des sous-traitants techniques et représentants juridiques. Il s'agissait principalement de bloquer les sites web de ces acteurs par le biais d'attaques DDoS et dans quelques cas de modifier la présentation des sites (*defacement*), voire de subtiliser des données et de les faire « fuiter » auprès du grand public (ainsi la correspondance interne du cabinet d'avocats ACS:Law fut-elle publiée, dévoilant les techniques contestables employées pour intimider les personnes ayant téléchargé des contenus protégés). Ces moyens furent ensuite redirigés vers une autre campagne baptisée « Avenge Assange », visant à défendre le fondateur de WikiLeaks qui, tout au long de l'année 2010, avait orchestré avec plusieurs grands médias internationaux une succession de « méga-fuites » de documents confidentiels. Dans le cadre de la répression exercée contre WikiLeaks, un certain nombre de services avaient cessé d'héberger les infrastructures techniques de l'organisation ou les comptes bancaires vers lesquels transitaient des dons financiers. Les Anonymous concentrèrent notamment leurs attaques sur les sites de MasterCard, Visa ou encore PayPal, qu'ils parvinrent à rendre brièvement inaccessibles.

Dans la foulée de cet épisode, les Anonymous furent également impliqués dans des actions liées aux Printemps Arabes, attaquant par exemple des sites web des gouvernements tunisien et égyptien. Mais la longue liste des entreprises conduites sous la bannière Anonymous comprend une grande diversité de cas de figure. Certaines sont de nature futile, comme celle visant à « punir » le site 9gag pour s'être « approprié » des mèmes issus de 4chan (« Operation Deepthroat », 2011). Beaucoup s'inscrivent dans la lignée de « Operation Payback » et visent des entreprises, organisations ou individus considérés comme abusant des droits de propriété intellectuelle ou menant une politique anti-piratage

trop agressive (Sony fut ainsi une cible récurrente). Mais d'autres se sont greffées sur des mouvements sociaux en cours, par exemple en soutien à Occupy Wall Street[9], ou encore lors des manifestations à Ferguson contre les violences policières racistes (« Op Ferguson », 2014). D'autres enfin relèvent de ce que les critiques internes appellent les « opérations de chevaliers blancs » (*white knight ops*). Elles incluent par exemple des attaques DDoS contre des sites pédopornographiques, et l'intrusion sur les serveurs pour collecter et diffuser les identifiants de leurs utilisateurs (« Operation DarkNet », 2011) ; la dénonciation publique d'auteurs de harcèlement, de violences sexuelles et de chantages suite au suicide de la jeune Amanda Todd au Canada (« OpAntiBully », 2012-2013) ; ou encore, l'identification des auteurs de viols en réunion à Steubenville dans l'Ohio, puis à Maryville dans le Missouri, ainsi que la diffusion de vidéos et de messages incriminants (« Op Roll Red Roll », 2012 et « Op Maryville », 2013)[10].

Anonymous ou les ruses de la visibilité : de l'action clandestine au dévoilement spectaculaire

Les objectifs ont donc varié mais le langage employé, bien que souvent ironique, relève du champ sémantique de la guérilla – le lieu par excellence de la ruse, utilisée par le faible contre le fort : des « opérations » coordonnées sont lancées, qui prennent parfois la forme d'assauts collectifs qualifiés de « raids » où les participants se déploient « en essaim » (*swarm*) contre leurs cibles. Dans certains cas il s'agit au préalable d'aller « enquêter » sur un événement, au besoin en s'introduisant dans des serveurs ou des ordinateurs. Ainsi, si certaines actions comportent une dimension tout à fait légale (publier des vidéos), d'autres se situent à la frontière de la légalité (diffuser des informations personnelles, qui peuvent être déjà accessibles par ailleurs), tandis que d'autres encore sont manifestement illégales (les attaques DDoS, les intrusions dans des systèmes d'information).

L'exemple ci-dessous (illustration 2) présente l'interface IRC d'une chaîne du réseau AnonOps évoqué plus haut, lors du lancement suite aux attentats de novembre 2015 d'une « OpParis », qui s'inscrit elle-même dans le contexte des « OpISIS » visant l'État Islamique. Dans le bandeau en haut de la page, on trouve les ressources de communication externes de l'opération (vidéos YouTube, comptes et hashtags sur Twitter), des instructions pour participer (« HowToHelp ») publiées sur un *pastebin*[11], et enfin la liste des « cibles » identifiées et diffusées sur un « pad » (éditeur de texte collaboratif). Les objectifs y figurent en rouge : « Lancer l'attaque, trouver des comptes/sites pro-ISIS, les "défigurer" [*deface*] et "déballer" des informations ou des données [*dump*] ! ».

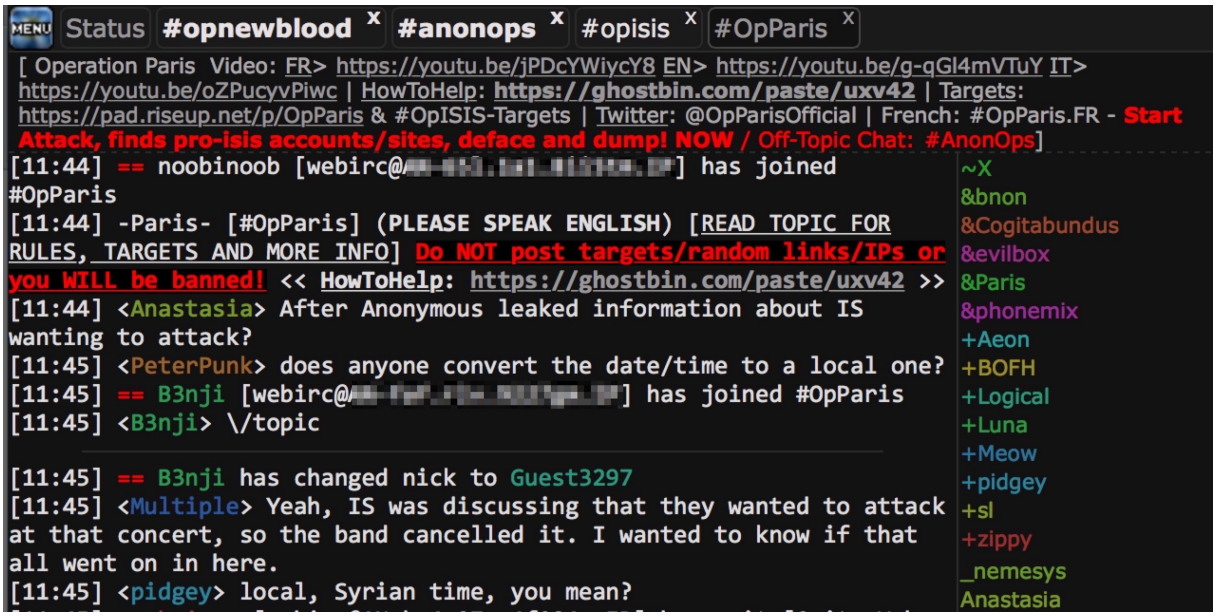

Illustration 2 : chaîne IRC dédiée à #OpParis, capture d'écran (les adresses de connexion ont été anonymisées), 27 novembre 2015

Sur le plan de la communication, il faut donc d'abord distinguer ce qui relève des échanges internes d'un côté, avec plusieurs niveaux de confidentialité : la socialisation sur le forum 4chan, dans certains cas la création de wikis ou de sites dédiés pour mettre des ressources à disposition, et surtout la coordination via les canaux IRC. Ces derniers constituent des arènes privilégiées permettant d'échanger avec les autres membres, de segmenter les tâches, mais aussi de constituer des « cellules » dédiées à certains objectifs, et qui peuvent parfois évoluer en factions dissidentes. De l'autre côté se situe la façade publique voire de « propagande » du mouvement, avec une communication externe destinée à envoyer des messages sous la forme de « communiqués » publiés sur des *pastebin,* de flyers et de pamphlets diffusés sous forme d'images, des vidéos sur YouTube, ou encore l'animation de comptes sur des plateformes telles que Twitter.

Sur le plan des actions elles-mêmes, on peut relever une gamme de techniques qui constituent le « *répertoire d'action numérique* » (Van Laer et Van Aelst, 2010 ; d'après Tilly 1984) des Anonymous. Si elles visent en de rares occasions à infliger des dommages (par exemple en modifiant ou en effaçant des données sur des serveurs), la grande majorité consiste à soumettre les cibles choisies à un *dévoilement spectaculaire* par un excès d'attention négative, en adoptant deux grands types d'approches (souvent combinées) : la première consiste à paralyser momentanément ou à occuper symboliquement un espace numérique ; la seconde implique de divulguer des informations personnelles ou confidentielles, qui peuvent porter atteinte à la réputation d'une personne ou d'une organisation, et qui peuvent servir à les identifier comme cibles.

Le premier mode d'intervention peut consister en de simples *détournements* destinés à « faire passer un message », l'une des solutions consistant à pénétrer sur un site web pour en « défigurer » le contenu (*defacement*) : il peut s'agir d'un graffiti sur la page d'accueil, ou bien d'accusations plus précises, comme lorsque les noms et photos de personnes décédées furent affichées sur le site européen de l'église de Scientologie en 2009, accompagné de la mention : « *Pourquoi sont-ils morts, Scientologie ?* ». D'autres formes d'actions qui relèvent du *raid* visent à produire un effet de *saturation*, qui peut être accompli par l'effet de nombre en « envahissant » une arène ou simplement par l'envoi massif de messages ou de coups de téléphone (le plus souvent de nature à choquer ou perturber les destinataires). C'est également la finalité de l'une des techniques de prédilection du mouvement à partir de 2010 avec la création du réseau IRC AnonOps : l'attaque par déni de service distribuée ou DDoS.

Dans un contexte d'activisme politique, ce type d'attaque a parfois été qualifié de « *sit-in* virtuel » et d'action de désobéissance civile, ce qui soulève de nombreuses questions (Sauter, 2014). Certaines sont assez classiques, dans la mesure où il s'agit de formes de blocage et d'empêchement – qui, bien que ponctuelles, peuvent être considérées comme illégitimes ; et qui en outre placent clairement leurs auteurs dans l'illégalité[12]. D'autres questions plus inédites relèvent de l'automatisation des processus, les attaques DDoS étant orchestrées en activant à distance des réseaux d'ordinateurs infectés ou *botnets* (qui peuvent compter des milliers voire des millions de machines)[13], afin de lancer des connexions en masse vers une IP donnée. Cette technique suppose d'être parvenu à constituer la ressource que constitue un *botnet*, dont l'efficacité et la puissance peuvent varier. Des *botnets* « volontaires » ont également pu être ajoutés, à partir d'applications permettant aux participants de joindre leur propre machine à l'attaque DDoS, notamment au moment de Operation Payback et Avenge Assange[14], contribuant à l'idée d'un mouvement collectif et légitimant la démarche. Mais il s'agissait le plus souvent d'actions pouvant être déclenchées par un nombre restreint de personnes et à peu de frais, tout en s'affichant comme l'expression de la « multitude ».

La seconde grande catégorie d'interventions consiste à divulguer des informations normalement peu ou pas accessibles. Il peut s'agir d'informations personnelles (noms, adresses, photos, numéros de téléphone, comptes sur les médias sociaux), parfois obtenues en s'immisçant dans des systèmes informatiques ou en trompant les interlocuteurs qui les détiennent (*social engineering*). On parle alors de *doxing* ou *doxxing* (de l'abréviation de documents « *docs* ») ou de *dump* (terme qui désigne normalement la copie de sauvegarde d'une base de données, mais qui dans ce contexte implique également une opération de « déballage »). Il peut aussi s'agir de données ou de documents compromettants pour des organisations, qui mettent au jour des injustices ou des pratiques contestables – dans ce cas on parlera plutôt de « fuites » (*leaks*).

Ce type d'actions, qui consiste à mettre sous le feu des projecteurs médiatiques des individus ou des comportements, implique des effets punitifs puissants puisqu'il s'agit de « nommer et humilier » (*name and shame*), et éventuellement de contraindre les autorités à agir. Leurs conséquences peuvent être dévastatrices, d'abord parce que les Anonymous peuvent fréquemment commettre des erreurs (dans le contexte des émeutes raciales de Ferguson par exemple, une personne fut identifiée à tort comme le policier responsable de la mort du jeune afro-américain Michael Brown), mais aussi parce qu'en ne maîtrisant pas tous les paramètres d'une situation locale, ils peuvent également surexposer les victimes avec des conséquences dramatiques (comme lors de l'Op Steubenville). Ils présentent enfin un paradoxe : dans le cas de l'OpAntiBully, les Anonymous dénoncent des pratiques de harcèlement (récurrentes sur 4chan par ailleurs…), tout en mobilisant ces mêmes pratiques pour punir leurs cibles dans le contexte d'une « culture de la vengeance éclair » (Stroud, 2016).

***

Comme le notent Detienne et Vernant : « *Pourquoi la mètis apparaît-elle ainsi multiple (*panloiè*), bigarrée (*poikilè*), ondoyante (*aiolè*) ? Parce qu'elle a pour champ d'application le monde du mouvant, du multiple, de l'ambigu. Elle porte sur des réalités fluides, qui ne cessent jamais de se modifier et qui réunissent en elles, à chaque moment, des aspects contraires, des forces opposées. (…) La victoire sur une réalité ondoyante, que ses métamorphoses continues rendent presque insaisissable, ne peut être obtenue que par surcroît de mobilité, une puissance encore plus grande de transformation.* » (1974, p. 27-28). L'environnement numérique constitue par essence un monde « fluide » et « ondoyant », sur lequel les Anonymous ont ponctuellement pris l'ascendant par une surenchère de fluidité, sans toutefois que ces actions viennent servir des objectifs de plus long terme. Il serait vain de chercher une cohérence idéologique chez les Anonymous, en dehors d'une interprétation maximaliste de la liberté de circulation de l'information. Les interventions visent le plus souvent à répondre à des « injustices » (réelles ou perçues) par des actions directes distribuées, qui s'affranchissent des formes instituées de la contestation pour privilégier des formes de dévoilement spectaculaire. Par les ruses décrites au cours de cet article, elles manifestent donc un certain opportunisme typique d'une démarche tactique par opposition à la planification stratégique (Certeau 1980) – dont elles peinent cependant à sortir pour produire un véritable sens politique.

Certaines initiatives que nous avons recensées relèvent de l'empêchement et s'inscrivent dans la lignée du « *sabotage électronique* » théorisé dès les années 1990 par le collectif Critical Art Ensemble (1997) comme mode de subversion actif. Elles peuvent également s'apparenter à des formes de « *détournement culturel* » rassemblées sous la notion de *culture jamming* (Dery 1993) ou de « *média tactique* » (Renzi 2008 ; Raley 2009). Celles-ci tiennent d'une modalité « carnavelesque » de la contestation (Bruner 2005) et d'une culture du canular (*pranksterism*). Mais d'autres types d'actions visent à dénoncer, harceler ou intimider des organisations ou des individus ciblés et constituent ainsi une modalité du *vigilantisme numérique* (Loveluck, 2016 ; 2020). Ce dernier comporte une dimension vindicative ou punitive, particulièrement lorsque ce sont des individus (et leur réputation) qui se trouvent publiquement mis en cause – sans possibilité de recours en cas d'erreur ou d'effets collatéraux non anticipés. Dans ces cas de figure, la frontière entre la défense d'une cause politique et l'affirmation d'une forme de justice expéditive sont ténues.

Les Anonymous se rassemblent autour d'actions qui sont autant de *projets* ponctuels, dont la continuité est d'abord établie par une « culture commune » d'initiés, puis par des signifiants qui peuvent être investis de manière très diverse mais qui permettent la constitution au cours du temps d'une identité collective publique, bien qu'instable et distribuée. Comme l'ont montré certains procès intentés à des membres après leur arrestation ainsi que l'analyse des rapports de pouvoir au sein du mouvement (Uitermark 2017), derrière un apparent « esprit en essaim » (*hive mind*) mis en scène par le mouvement ainsi que l'unité affichée autour d'une iconographie et de pratiques partagées, les actions les plus sophistiquées et ciblées sont généralement menées par des sous-groupes beaucoup plus restreints – permettant une coordination plus efficace et une communication plus homogène. Les revendications de

représenter le « peuple » d'internet de manière ouverte, explicitement décentralisée et non-hiérarchique sont donc soumises à caution, et apparaissent là encore comme une forme d'illusion spectaculaire.

Si le coup d'éclat ou le « raid » n'avaient initialement qu'une motivation intrinsèque de divertissement, à l'épreuve de leur succès médiatique les acteurs du mouvement ont été tenus d'apporter des justifications à leurs actions – et proposer un cadre et une finalité au nouveau pouvoir qu'ils avaient découvert. Le nombre de participants et leur capacité de nuisance ont souvent été exagérés, mais ils sont révélateurs de la place prise par le mouvement dans l'imaginaire collectif – bien qu'aujourd'hui le masque ne suscite plus le même engouement. La ruse a donc peut-être consisté avant tout à produire une image capable de capter l'attention et d'occuper l'espace médiatique, tout en édifiant une forme de supériorité morale. En jouant avec la figure de la multitude vengeresse, les actions entreprises ont donné l'apparence d'une subjectivité populaire œuvrant à rendre la justice. Le masque est ainsi devenu l'un des marqueurs de la contestation politique – et alors que le mouvement lui-même est aujourd'hui largement en sommeil, on peut encore parfois l'apercevoir lors de manifestations publiques. Dans le même temps, les ruses de la visibilité inaugurées par Anonymous se sont diffusées voire banalisées, continuant à brouiller les contours de l'action politique en régime numérique, entre expression militante et désir de justice directe.

Références

M. S. Bernstein *et al*., « 4chan and /b: an analysis of anonymity and ephemerality in a large online community », *5th International AAAI Conference on Weblogs and Social Media*, Barcelone, 2011.

Y. Benkler, « Hacks of valor. Why Anonymous is not a threat to national security », *Foreign Affairs,* 4 avril 2012.

D. M. boyd, « "for the lolz": 4chan is hacking the attention economy », *Apophenia,* blog personnel, 12 juin 2010 (http://www.zephoria.org/thoughts/archives/2010/06/12/for-the-lolz-4chan-is-hacking-the-attention-economy.html).

M. L. Bruner, « Carnivalesque protest and the humorless state », *Text and Performance Quarterly* vol. 25, n° 2, 2005, p. 136-155.

M. de Certeau, *Arts de faire : l'invention du quotidien*, Paris, Gallimard, 1980.

G. Coleman, « Phreaks, hackers, and trolls. The politics of transgression and spectacle », in M. Mandiberg (dir.), *The Social Media Reader*, New York and London, New York University Press, 2012, p. 99-119.

G. Coleman, *Anonymous. Hacker, activiste, faussaire, mouchard, lanceur d'alerte*, Montréal, Lux éditeur, 2016.

G. Coleman, « Logics and legacy of Anonymous », in J. Hunsinger, M. M. Allen, et L. Klastrup (dir.), *Second International Handbook of Internet Research*, Dordrecht and London, Springer, 2020, p. 145-166.

M. Detienne et J.-P. Vernant, *Les Ruses de l'intelligence. La mètis des Grecs*, Paris, Flammarion, 1974.

C. A. Ensemble, *La Résistance électronique, et autres idées impopulaires*, Paris, Ed. de l'Eclat, 1997.

M. Dery, *Culture Jamming. Hacking, Slashing and Sniping in the Empire of Signs*, Westfield, NJ, Open Media, 1993.

A. Golub, « Being in the World (of Warcraft): raiding, realism, and knowledge production in a massively multiplayer online game », *Anthropological Quarterly* vol. 83, n° 1, 2010, p. 17-45.

M. Hardt et A. Negri, *Empire*, Paris, Exils, 2000.

G. E. Hine *et al*., « Kek, cucks, and God Emperor Trump: a measurement study of 4chan's politically incorrect forum and its effects on the Web », *ICWSM - International Conference on Web and Social Media*, 2017.

T. Jordan, *Activism! Direct Action, Hacktivism and the Future of Society*, London, Reaktion Books, 2001.

T. Jordan et P. A. Taylor, *Hacktivism and Cyberwars. Rebels With A Cause?*, London and New York, Routledge, 2004.

T. Jordan, *Hacking. Digital Media and Technological Determinism*, Cambridge and Malden, MA, Polity Press, 2008.

A. G. Klein, « Vigilante media: unveiling Anonymous and the hacktivist persona in the global press », *Communication Monographs* vol. 82, n° 3, 2015, p. 379-401.

G. Latzko-Toth, « L'Internet Relay Chat : un cas exemplaire de dispositif sociotechnique », *Commposite* vol. 4, n° 1, 2008, p. 52-73.

B. Loveluck, « Le vigilantisme numérique, entre dénonciation et sanction. Auto-justice en ligne et agencements de la visibilité », *Politix* vol. 29, n° 115, 2016, p. 127-153.

B. Loveluck, « The many shades of digital vigilantism. A typology of online self-justice », *Global Crime* vol. 21, n° 3-4, 2020, p. 213-241.

K. McDonald, « From Indymedia to Anonymous: rethinking action and identity in digital cultures », *Information, Communication & Society* vol. 18, n° 8, 2015, p. 968-982.

A. Nagle, *Kill All Normies. Online Culture Wars From 4Chan and Tumblr to Trump and the Alt-Right*, Winchester, Zero Books, 2017.

A. Nissenbaum et L. Shifman, « Internet memes as contested cultural capital: the case of 4chan's /b/ board », *New Media & Society* vol. 19, n° 4, 2017, p. 483-501.

W. Phillips et R. M. Milner, *The Ambivalent Internet. Mischief, Oddity, and Antagonism Online*, Cambridge and New York, Polity, 2017.

W. Phillips, *This Is Why We Can't Have Nice Things. Mapping the Relationship Between Online Trolling and Mainstream Culture*, Cambridge, MA, MIT Press, 2015.

C. Poole, « The case for anonymity online », *TED Talks,* vidéo, février 2010 (http://www.ted.com/talks/christopher_m00t_poole_the_case_for_anonymity_online.html).

R. Raley, *Tactical Media*, Minneapolis, MN, University of Minnesota Press, 2009.

A. Renzi, « The space of tactical media », in M. Boler (dir.), *Digital Media and Democracy. Tactics in Hard Times*, Cambridge, MA, MIT Press, 2008, p. 71-100.

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

S. R. Stroud, « "Be a bully to beat a bully": Twitter ethics, online identity, and the culture of quick revenge », in A. Davisson et P. Booth (dir.), *Controversies in Digital Ethics*, New York and London, Bloomsbury, 2016, p. 264-278.

C. Stryker, *Epic Win for Anonymous. How 4chan's Army Conquered the World*, New York, Overlook Press, 2011.

C. Tilly, « Les origines du répertoire d'action collective contemporaine en France et en Grande-Bretagne », *Vingtième Siècle. Revue d'histoire* vol. 4, n° 4, 1984, p. 89-108.

J. Uitermark, « Complex contention: analyzing power dynamics within Anonymous », *Social Movement Studies* vol. 16, n° 4, 2017, p. 403-417.

J. Van Laer et P. Van Aelst, « Internet and social movement action repertoires. Opportunities and limitations », *Information, Communication & Society* vol. 13, n° 8, 2010, p. 1146-1171.

[1] Le hacker Jeremy Hammond fut ainsi arrêté en 2012 et condamné à 10 ans de prison pour s'être introduit dans le système d'information de l'entreprise privée de renseignement Stratfor, et avoir dérobé puis diffusé via WikiLeaks leur correspondance email – divulguant ainsi la liste de leurs clients et la nature de leurs relations, ainsi que la surveillance effectuée par exemple à l'encontre du mouvement Occupy Wall Street.

[2] LulzSec ou Lulz Security est un groupe dont une partie des membres émanait d'Anonymous, qui a lancé une longue série d'attaques informatiques très médiatisées en mai-juin 2011. Avec leur compte Twitter très suivi, leur sémiologie décalée (un logo consistant en un personnage en haut-de-forme avec un monocle et un verre de vin à la main, la musique de la série « La croisière s'amuse » sur leur site web etc.) et la tonalité sarcastique de leurs interventions, LulzSec annonçait initialement vouloir rétablir l'esprit de dérision et de moquerie (« *lulz* ») contre un militantisme politique qui se prendrait trop au sérieux. Leurs intrusions et blocages de sites manifestaient un plus haut degré de sophistication que celles attribuées à Anonymous, et ont entraîné une réponse plus ferme des autorités qui ont finalement arrêté la plupart des membres du noyau du groupe, composé d'environ 7 personnes. Enfin on apprit plus tard que le fondateur du groupe « Sabu » (Hector Monsegur) avait été contraint de devenir informateur pour le FBI, leur permettant d'arrêter d'autres membres de LulzSec ainsi que d'Anonymous.

[3] Ce qui n'empêchera pas le jeune homme de quitter 4chan et d'être recruté en 2016 par Google.

[4] AnonOps fut créé en 2010 suite aux difficultés rencontrées lors d'une action collective d'envergure destinée à « faire payer » les éditeurs et ayants droit luttant contre le piratage de contenus audiovisuels (« Operation Payback »), afin de garantir la sécurité des communications et l'anonymat des participants et, selon les termes de ses administrateurs, favoriser « la libre discussion des idées » (voir https://www.anonops.com/about.html). Ce réseau IRC est demeuré jusqu'en 2015 la principale matrice des opérations lancées par les Anonymous.

[5] « Nous sommes Anonymous. Nous sommes légion. Nous ne pardonnons pas. Nous n'oublions pas. Comptez sur nous ». Voir « Message to Scientology », *YouTube*, 21 janvier 2008 (https://www.youtube.com/watch?v=JCbKv9yiLiQ, consulté le 1er mars 2018).

[6] Le masque est porté par le personnage principal, qui évolue dans un contexte dystopique où un parti fasciste a pris le pouvoir. Ce mystérieux opposant anarchiste est censé représenter Guy Fawkes, l'un des principaux membres de la Conspiration des poudres dirigée contre le roi d'Angleterre et le Parlement en 1605.

[7] Voir par exemple Damien Leloup, « LulzSec, l'ascension éclair d'un groupe de pirates informatiques », *Le Monde.fr*, 24 juin 2011 (http://www.lemonde.fr/technologies/article/2011/06/24/lulzsec-l-ascension-eclair-d-un-groupe-de-pirates-informatiques_1540672_651865.html, consulté le 1er mars 2018).

[8] Pour une liste non exhaustive, voir la page suivante : https://en.wikipedia.org/wiki/Timeline_of_events_associated_with_Anonymous

[9] En aidant à l'organisation et à la communication, mais aussi par exemple en diffusant les informations personnelles d'un policier accusé d'avoir aspergé des manifestants pacifiques avec du gaz lacrymogène à l'Université de Californie à Davis en 2011.

[10] Voir Emily Bazelon, « The online avengers », *The New York Times*, 15 janvier 2014 (http://www.nytimes.com/2014/01/19/magazine/the-online-avengers.html, consulté le 1er mars 2018).

[11] Souvent utilisés en conjonction avec les canaux IRC, de tels sites permettent de « déposer » des quantités importantes de texte (initialement du code informatique à évaluer entre développeurs de logiciels) pour un affichage public, sans encombrer les discussions. Ils ont été détournés de leur fonction première pour la publication de tels communiqués, où pour diffuser des fuites de données (*data leaks*) ou des informations personnelles (*doxing*).

[12] Et ce d'autant que les actions de désobéissance civile impliquent normalement d'agir à découvert, la violation de la loi et l'arrestation qui en découlent faisant partie intégrante de la démarche.

[13] Les sites les plus exposés se sont désormais protégés et pour être efficace, ce type d'attaque nécessite aujourd'hui des *botnets* très puissants.

[14] Ce type de programme, initialement connu sous le nom de LOIC (pour *Low Orbit Ion Cannon*), ne protégeait pas suffisamment ses utilisateurs et permit un certain nombre d'arrestations.