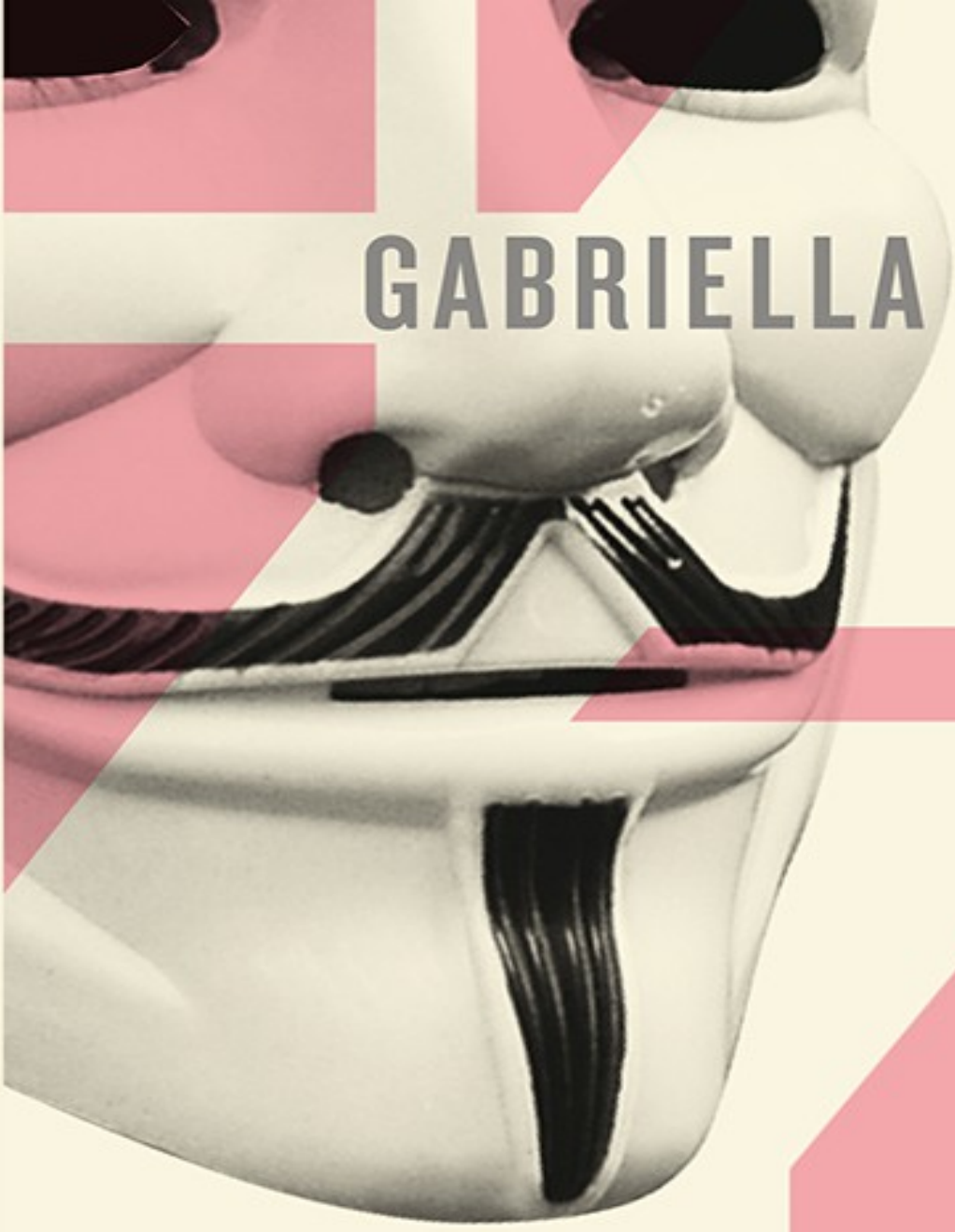
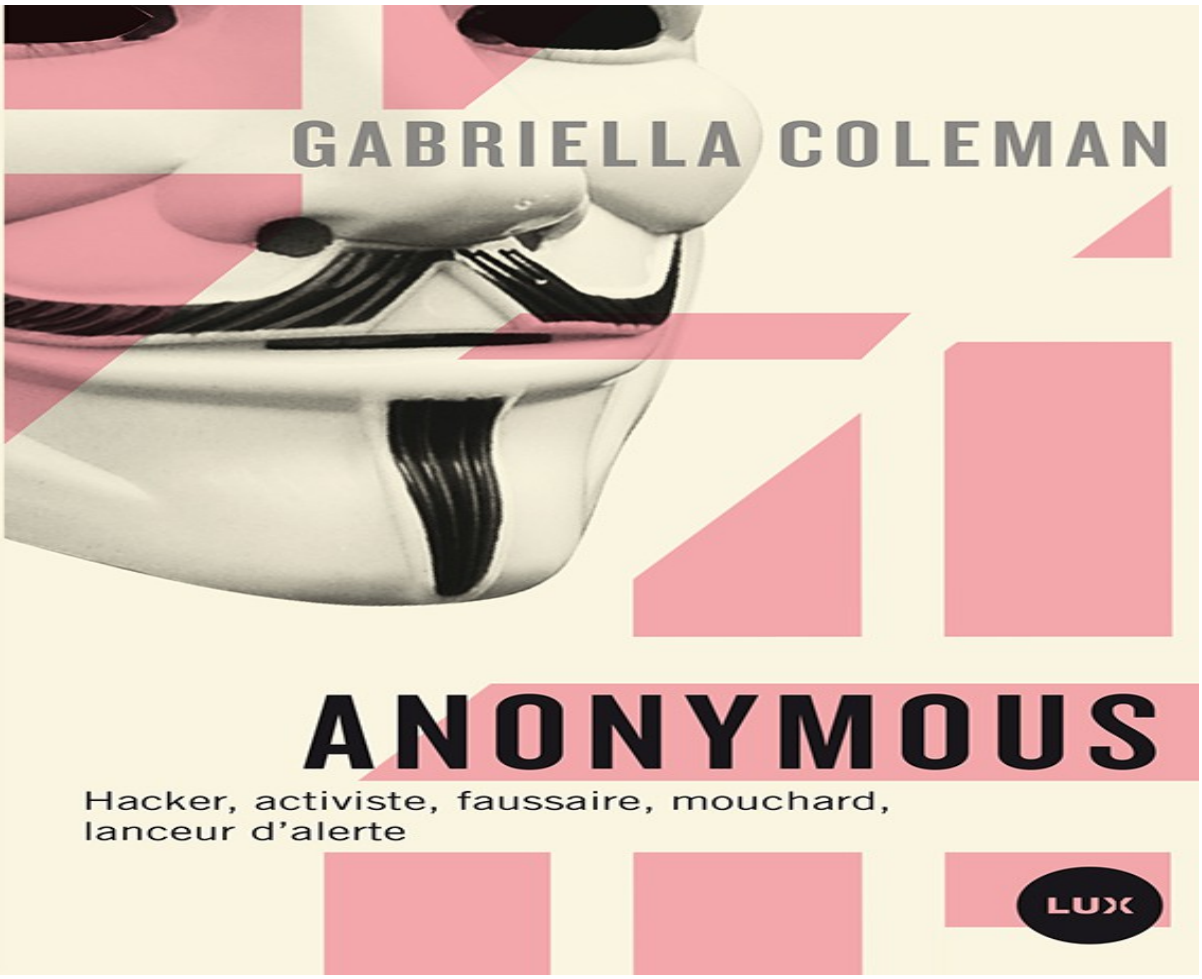


GABRIELLA COLEMAN

ANONYMOUS

Hacker, activiste, faussaire, mouchard,
lanceur d'alerte

LUX


GABRIELLA COLEMAN
ANONYMOUS
Hacker, activiste, faussaire, mouchard,
lanceur d'alerte
LUX

Clique ici pour plus de livres : https://t.me/formations8

ANONYMOUS

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

GABRIELLA COLEMAN

ANONYMOUS

Hacker, activiste, faussaire, mouchard, lanceur d'alerte

Traduit de l'anglais
par Nicolas Calvé

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

© Lux Éditeur, 2016
www.luxediteur.com

Conception graphique de la couverture: David Drummond

Dépôt légal: 1er trimestre 2016
Bibliothèque et Archives Canada
Bibliothèque et Archives nationales du Québec
ISBN (papier): 978-2-89596-207-6
ISBN (epub): 978-2-89596-683-8
ISBN (pdf): 978-2-89596-883-2

Ouvrage publié avec le concours du Programme de crédit d'impôt du gouvernement du Québec et de la SODEC. Nous reconnaissons l'aide financière du gouvernement du Canada par l'entremise du Fonds du livre du Canada (FLC) pour nos activités d'édition, ainsi que du Programme national de traduction pour l'édition du livre, une initiative de la *Feuille de route pour les langues officielles du Canada 2013-2018: éducation, immigration, communautés*, pour nos activités de traduction.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Je dédie ce livre aux légions d'Anonymous
celles qui ont revêtu le masque hier
celles qui osent se tenir debout aujourd'hui
celles qui sans doute se soulèveront demain

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

«Vous avez désormais notre attention»

Le 29 juillet 2007, une entité disant s'appeler Anonymous (un nom alors inconnu de tous, sauf des internautes les mieux informés) poste une vidéo sur YouTube. Un homme sans tête apparaît sur un fond blanc, en costume. «Cher Fox News», commence une voix synthétique au timbre métallique. Peu de temps auparavant, la chaîne d'information a consacré tout un segment d'une émission à un groupe qu'elle a appelé «la machine de haine d'internet» (*the Internet Hate Machine*), une appellation que le collectif arborera ultérieurement comme titre d'honneur[1].

Or pour un groupe qui se repaît de tromperie et de malice, se contenter de tourner en dérision un tel exposé reviendrait à rater une occasion en or de se faire plaisir. Sur un ton solennel et peu rassurant, la voix grave poursuit ainsi son discours:

> Le nom et la nature d'Anonymous ont été souillés comme une putain dans une ruelle, puis livrés au regard du public. Permettez-moi d'affirmer ceci sans détour: vous n'avez absolument pas compris qui nous sommes et ce que nous sommes. [...] Nous sommes tout le monde et nous ne sommes personne. [...] Nous sommes le visage du chaos et les annonciateurs du jugement. Nous rions devant la tragédie. Nous nous moquons de ceux qui souffrent. Nous ruinons la vie d'autrui pour la seule raison que nous en avons la capacité. [...] Un

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> homme se défoule sur un chat, nous rions. Des centaines de personnes meurent dans un accident d'avion, nous rions. Nous sommes l'incarnation d'une humanité sans remords, sans empathie, sans morale.

Puis, la vidéo se termine: «Vous avez désormais... *notre* attention.»

En tout cas, ils ont certainement la mienne. Peu de temps après la diffusion de la vidéo, je me suis embarquée pour plusieurs années dans un projet de recherche sur le collectif, une tâche colossale que je viens tout juste d'achever (et que ce livre concrétise). La vidéo se voulait une satire du discours hyperbolique de Fox News, qui présentait les membres d'Anonymous comme les vecteurs par excellence des mauvais coups et de la calomnie sur internet, comme des «hackers[*] dopés aux stéroïdes». Et pourtant, l'atmosphère à glacer le sang qui s'en dégage ne pourrait mieux exprimer ce que les trolls* ont de terrifiant. Au lieu de réfuter le portrait ridiculement tendancieux de Fox News, la vidéo le corrobore entièrement – mais seulement pour ceux qui ne voient pas la plaisanterie, bien sûr.

Ce double sens résume très bien l'humour noir dont Anonymous a fait sa spécialité (que ses membres appellent le *lulz**). Comme nous le verrons dans ces pages, le *lulz*, à la fois humour déviant et état quasi mystique, a évolué avec Anonymous depuis sa naissance. À ses débuts, le groupe ne semblait chercher qu'à semer la pagaille dans l'esprit du *lulz*. Cependant, peu après la diffusion de cette vidéo parodique et grandiloquente, on a commencé à voir des Anons* au cœur de centaines d'actions politiques, ceux-ci devenant même parties prenantes de certaines des luttes les plus décisives de notre époque. En janvier 2011, en solidarité avec les insurgés de Tunisie, Anonymous a hacké les sites web du gouvernement tunisien; quelques mois plus tard, des *indignados* espagnols ont projeté le masque emblématique de Guy Fawkes sur un immeuble de la Puerta del Sol; aux États-Unis, des Anons ont été parmi les premiers à faire circuler les appels à occuper Wall Street.

C'est que le collectif, les années précédentes, s'était petit à petit affirmé comme force sociale et politique avec une série d'actions, dont

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

certaines comptent parmi ses plus mémorables. En 2008, des membres qui souhaitaient renouveler la mission d'Anonymous ont pris à partie l'Église de scientologie après que cette organisation controversée eut tenté d'empêcher la diffusion d'une vidéo virale de Tom Cruise. Élaborée dans l'esprit du *lulz*, l'opération a permis aux Anons de concrétiser leur pouvoir d'influer sur des luttes à l'échelle mondiale, tout en goûtant à l'euphorie de l'engagement. Deux ans plus tard, soit en décembre 2010, Anonymous a accédé à une notoriété encore plus grande avec l'opération Avenge Assange (venger Assange). À l'initiative d'AnonOps, un des nœuds les plus activistes et les plus prolifiques du collectif, des Anons se sont lancés dans l'action directe en déclenchant une campagne d'attaques informatiques par saturation (*distributed denial-of-service*, DDoS)*. La tactique, qui consiste à bloquer l'accès à des serveurs web en les submergeant de requêtes, visait des institutions financières qui refusaient de traiter les dons à WikiLeaks, dont PayPal et MasterCard. Anonymous est sorti plus fort de chacune de ces opérations.

Néanmoins, même si Anonymous s'est distancié de l'ingouvernable chaos de la nuisance pure pour s'engager dans le débat politique mondial, ses interventions militantes, qu'elles prennent la forme de manifestations de rue ou d'intrusions informatiques spectaculaires, suscitent invariablement la même question: les membres d'Anonymous sont-ils des dissidents qui défendent certains principes, ou une bande de gamins désœuvrés qui, shootés au *lulz*, glandent sur internet?

Cette ambivalence est tout à fait compréhensible. Car au-delà de son combat fondateur pour le maintien de l'anonymat et la libre circulation de l'information, Anonymous ne défend ni philosophie ni programme politique cohérents. Bien que le collectif soit reconnu pour sa contestation dans l'univers numérique et ses actions directes, il n'a jamais affiché d'orientation claire. Parce qu'Anonymous trouve son origine dans l'univers parfois humoristique, souvent irrévérencieux et par moments très envahissant des trolls du web (dont la logique semble de prime abord peu propice au développement d'une culture militante et politique), il est frappant de constater que des activistes en viennent à s'en réclamer.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

De trolls à désaxés de la scène militante

Aujourd'hui, le rayonnement du masque de Guy Fawkes et des idées qu'il a fini par symboliser, jusque chez les manifestants de la place Tahrir ou les parlementaires polonais opposés à l'Accord commercial anticontrefaçon (mieux connu sous son acronyme anglais ACTA, pour Anti-Counterfeiting Trade Agreement), peut paraître absurde à qui connaît les origines d'Anonymous. Avant 2008, le nom servait presque exclusivement à ce qu'un Anon a qualifié de «salopage sur internet» (*Internet motherfuckery*). Né dans les recoins du forum /b/ de 4chan (souvent considéré comme le «trou du cul du net»), Anonymous était synonyme de «troll» – terme désignant toute activité visant à salir la réputation d'individus ou d'organisations et à divulguer des données privées dans le but de nuire. Les trolls cherchent à contrarier les gens en diffusant des contenus sinistres ou répugnants, en semant la zizanie ou la pagaille. Ils peuvent martyriser leur proie en adoptant des identités, des croyances et des valeurs pour leur seul potentiel malfaisant, en saturant les forums de discussions de pourriels, en envoyant des centaines de pizzas, des taxis ou même une escouade tactique à la résidence visée. Quelle que soit la technique utilisée, les trolls se plaisent à dire qu'ils font ce qu'ils font pour le *lulz*, terme dérivé de *lol** désignant une forme d'humour grinçant, souvent malveillant.

Un des premiers raids (maintenant légendaire) des trolls d'Anonymous a visé une plateforme virtuelle appelée Habbo Hotel, dont le slogan clame avec enthousiasme «Crée ton avatar, décore ton appart, chatte et fais-toi plein d'amis». Conçu en Finlande, le site s'adresse aux pré-adolescents. Ceux-ci sont invités à se créer de mignons petits avatars à l'allure de Legos, qui peuvent socialiser dans l'hôtel et décorer leur chambre avec du «mobi». Le 6 juillet 2006, des Anons se sont connectés en grand nombre, prenant tous l'apparence d'hommes noirs arborant afro et complet gris. En manœuvrant avec adresse, ils ont réussi à former des swastikas humains et des piquets de grève pour empêcher les membres ordinaires (surtout des

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

enfants) d'accéder à la piscine de l'hôtel. Quiconque demandait les raisons qui motivaient ces gestes se voyait répondre par ces personnages à moustache que la piscine était fermée «pour cause de faillite et de sida».

Quelques années après les premiers raids contre Habbo, et à peine six mois après qu'on eut qualifié leur collectif de «machine de haine d'internet», des Anons ont commencé à organiser des actions politiques au nom d'Anonymous en affichant certains de ses éléments iconographiques (en particulier des hommes sans tête vêtus de complets noirs). Cette étonnante métamorphose s'est produite lors de ce que beaucoup d'observateurs considèrent aujourd'hui comme une des opérations de provocation les plus mémorables d'Anonymous: la campagne contre l'Église de scientologie. «De manière inédite, la communauté élargie des Anons s'est unie pour lancer un retentissant "Va te faire foutre!" à tout l'empire sectaire de la Scientologie[2]», raconte un participant. Motivés par le *lulz*, par le désir de provoquer une avalanche de dégâts aussi hilarants que terribles, des milliers d'Anons sont montés à bord d'un *troll train** baptisé «Project Chanology» en vue de lancer des attaques par saturation, d'envoyer des pizzas et des prostituées (non payées) à des églises de la secte un peu partout en Amérique du Nord, d'y faxer des images de parties du corps nues et de les submerger de canulars téléphoniques, en particulier les lignes spéciales de la Dianétique, conçues pour donner des conseils aux fidèles à propos de «la première technologie de l'esprit qui fonctionne».

On pouvait s'attendre à ce que, comme la plupart des raids précédents, ce retentissant «Va te faire foutre!» finisse par s'essouffler au bout de quelques jours d'espièglerie aussi féroces que ludiques. C'était sans compter sur une vidéo qu'un petit groupe de participants avait créée pour le seul plaisir du *lulz*, mais dont la diffusion a suscité de vifs débats entre les membres d'Anonymous. Dans le clip, on «déclarait la guerre» à l'Église de scientologie: «Pour le bien de vos fidèles, pour le bien de l'humanité – et pour notre plus grand plaisir. Nous allons vous expulser d'internet et procéder au démantèlement de l'Église de scientologie sous sa forme actuelle[3].» Après les avoir poussés au débat, cette déclaration ironique finirait par propulser les Anons dans la rue: le 10 février 2008, plus de

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

7 000 personnes ont manifesté dans 127 villes contre l'Église de scientologie, les violations des droits de la personne qu'elle commet et la censure qu'elle exerce.

C'est ainsi qu'Anonymous est passé du «salopage ultracoordonné sur internet» (comme l'expliquerait plus tard un Anon à mes étudiants) à la diffusion d'informations compromettantes sur l'Église de scientologie. Les Anons ont également tissé des liens avec des contestataires plus âgés qui dénonçaient déjà les agissements de la secte. Aux trolls succédait un engagement sincère, comme si Anonymous avait quitté son sanctuaire numérique pour travailler à la création d'un monde meilleur. Au cours des deux années qui ont suivi, des membres ont mis sur pied des groupes politiques indépendants d'Anonymous, et de nombreux participants en sont venus à se considérer comme d'authentiques militants, mais avec une tournure d'esprit transgressive.

Bon nombre des interventions d'Anonymous, dont ces vidéos qui ont fini par devenir une véritable institution, sont parfaitement légales. Cependant, une partie des tactiques du collectif, notamment les attaques par saturation et le hacking, sont illégales: en toutes circonstances, elles sont considérées comme des infractions criminelles, du moins aux États-Unis. Par conséquent, les autorités ont tenté par divers moyens de ranger certaines de ces opérations dans la catégorie générique de «cyberguerre» et d'intenter des poursuites judiciaires contre les personnes qui les ont menées. Le 21 février 2012, le *Wall Street Journal* a mis au jour cette stratégie en rapportant que, au cours de réunions secrètes, le général Keith Alexander, alors directeur de la National Security Agency (NSA), avait fait part à de hauts fonctionnaires de la Maison-Blanche de sa crainte qu'Anonymous «puisse avoir la capacité, d'ici un an ou deux, de provoquer une panne de courant limitée en menant une cyberattaque[4]».

En faisant son chemin dans les médias sociaux, l'article du *Wall Street Journal* a soulevé bien des questions. L'affirmation d'Alexander était-elle crédible? En quoi consistait précisément cette «capacité» de provoquer une panne? Si la menace était bien réelle, quelle serait la réponse adéquate? On ne saura sans doute jamais si l'évaluation de la NSA reposait sur des

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

renseignements fiables ou si elle visait simplement à jeter le discrédit sur Anonymous. Quoi qu'il en soit, le général Alexander est parvenu, au moins pour un temps, à dépeindre Anonymous comme un danger comparable aux djihadistes islamistes ou aux communistes d'autrefois.

En définitive, toutefois, le discours de la NSA s'est avéré peu convaincant. Malgré la grande diversité de ses tactiques – légales ou non, en ligne ou hors-ligne –, Anonymous n'a jamais appelé publiquement à commettre de tels attentats. Et rien n'indique que le collectif puisse aller jusqu'à l'envisager. Même dans leurs séances de chat les plus tumultueuses, ses membres n'ont jamais évoqué la possibilité de mettre des vies humaines en danger. Dans les reportages ultérieurs sur le sujet, des militants et des experts en sécurité ont d'ailleurs rejeté les allégations de la NSA en qualifiant ses propos d'«alarmistes[5]».

Même si Anonymous n'est pas du genre à recourir à une tactique comme celle-là, ses rapports avec le tribunal de l'opinion demeurent ambivalents. Ses méthodes sont parfois subversives, souvent vindicatives, généralement imprévisibles et habituellement peu respectueuses des convenances ou de la loi. Prenons l'exemple du *doxing**: la divulgation de données privées (numéro de sécurité sociale, adresse du domicile, photos, etc.) se situe dans une zone grise, car une partie des informations diffusées se trouve déjà sur des sites accessibles au public.

Une opération particulière d'Anonymous peut chevaucher les trois catégories (légalité, illégalité, zone grise) et, si les Anons peuvent y ajouter du *lulz*, ils ne s'en priveront pas. L'opération BART d'août 2011 en offre un bon exemple. Les membres du collectif ont senti la nécessité d'agir lorsqu'ils ont appris que les autorités du Bay Area Rapid Transit (BART, le métro de San Francisco) envisageaient d'interrompre le service de téléphonie mobile sur les quais de certaines stations en vue d'empêcher la tenue d'une manifestation contre la brutalité policière. Cette dernière avait été convoquée par des militants locaux pour dénoncer le meurtre par balles d'un passager, Charles Hill. Révoltés par cette ingérence de la société de transport dans le débat démocratique, les Anons ont donc participé à l'organisation d'une série de rassemblements.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Quelques membres se sont aussi introduits dans le système informatique du métro en vue de recueillir et diffuser des données sur les clients pour attirer l'attention des médias. L'un d'eux est tombé sur une photo osée du porte-parole officiel du BART, Linton Johnson, à demi nu, sur son site personnel. Le cliché a été publié sur un site appelé *Bartlulz*, accompagné d'une justification pour le moins impudente: «*If you are going to be a dick to the public, then I'm sure you don't mind showing your dick to the public.*» («Si tu fais le con [*dick*] avec le public, j'imagine que tu n'as pas peur de montrer ta bite [*dick*] au public.») Parfois fuyants et espiègles, parfois sérieux et inspirants, souvent tout cela à la fois (comme l'a démontré l'opération BART), ces mauvais plaisantins (*tricksters**, voir ici) sont animés, encore aujourd'hui, par une volonté de raillerie, par le *lulz*.

«Je l'ai fait pour le *lulz*»

L'insatiable appétit des Anons pour les espièglerie motivées par le *lulz* a-t-il, pour autant, fait de mon travail de recherche sur ce collectif une partie de plaisir? C'est dans le but de comprendre leur étonnante transformation de trolls marginaux en activistes excentriques que je me suis lancée dans l'étude anthropologique de ce groupe en 2008. J'ai entrepris mon travail dans la discrétion, sans détour, le cœur léger. Je prenais part à leurs manifestations et suivais leurs discussions sur les forums web et Internet Relay Chat (IRC), un des protocoles de communication les plus utilisés par Anonymous (et d'autres geeks* et hackers).

En 2011, alors qu'Anonymous étendait ses tentacules et que ses militants lançaient des actions politiques par dizaines, j'en suis venue à consacrer tout mon temps à ce projet initialement parallèle. Pendant plus de deux ans, j'allais être branchée en permanence. En ligne au moins cinq heures par jour, je me suis efforcée de me tenir au courant de toutes les opérations qui se déroulaient simultanément, bien que certaines m'aient été cachées en raison de leur nature clandestine. Enquêter sur Anonymous, c'était tenter de ne pas perdre le fil au travers d'un sentier sombre et

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

tortueux, jonché de rumeurs, de mensonges et de secrets, sans oublier la sinistre présence d'espions et d'informateurs. Mon parcours n'a pas manqué d'émotions fortes et de culs-de-sac enrageants. J'ai été témoin de toutes sortes de contorsions morales, les questionnements éthiques – en apparence insolubles – des Anons cohabitant sans peine avec leur goût du risque et leur sens exalté du sacrifice. Le collectif possède une structure organisationnelle qui, à l'instar des conséquences de ses actions, se révèle complexe et déroutante. Au fil du temps, j'ai pu constater qu'Anonymous n'a rien d'un labyrinthe dont on pourrait saisir la configuration et la sortie en le regardant d'en haut. La réalité est beaucoup plus complexe. Ce labyrinthe n'a rien de celui, statique, que Dédale avait créé pour enfermer le Minotaure. Il s'agit plutôt d'une machine infinie qui actionne une boucle récursive serrée, où des labyrinthes engendrent des labyrinthes eux-mêmes générateurs de labyrinthes.

Malgré les difficultés que j'ai rencontrées en explorant ce dédale infini, j'ai appris, peu à peu, à connaître Anonymous, tout comme ses membres ont appris à me connaître, personnellement pour certains d'entre eux. Comme l'aurait fait tout anthropologue, j'ai observé, écouté, interviewé, débattu, interrogé, incité. Par moments, j'ai même participé, tant que je restais dans les limites de la légalité. J'ai effectué des tâches très diverses, tel que réviser des manifestes, indiquer à des journalistes comment trouver Anonymous, rectifier de fausses informations.

Mon engagement respectait cependant des limites, volontaires et imposées par des contraintes extérieures. L'anthropologie exige à la fois le maintien d'une certaine distance et la capacité de pénétrer les choses en profondeur. L'astuce consiste à s'intégrer au groupe étudié tout en évitant de se borner aux interprétations que ses membres donnent des situations. Bon nombre des causes et des tactiques d'Anonymous me sont sympathiques, mais pas toutes. Divers scrupules d'ordre moral ont creusé une certaine distance critique. En raison de leur illégalité, certaines actions excédaient mes limites. Tant pour Anonymous que pour moi, il valait mieux que je n'y participe pas. Plus tard, après les arrestations et les

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

condamnations, j'ai pu me renseigner sur des opérations dont je n'avais rien su.

Avec le foisonnement des tactiques militantes au sein d'un nouveau groupe d'Anons pendant l'été 2011, la donne a changé. Anonymous s'en prendrait désormais aux sociétés figurant au palmarès Fortune 500 et aux fournisseurs de la Défense. Des hackers mercenaires se sont mis à transmettre des données privées d'Anons aux autorités – nom, photos, adresse. De leur côté, ceux-ci ont commencé à divulguer des informations confidentielles ou gênantes. C'est à ce moment-là que le Federal Bureau of Investigation (FBI) est entré en scène. Dans ces circonstances, peu importe la quantité de *lulz* qu'Anonymous injectait dans une opération, l'humour ne pouvait empêcher la progression d'un étouffant sentiment de malaise chez les membres et les observateurs du collectif. Ainsi, même si mes recherches sur Anonymous étaient souvent passionnantes – et constituaient sans aucun doute une véritable aventure –, j'ai été peu à peu gagnée par la paranoïa.

Telle une perturbation barométrique annonçant une tornade, la paranoïa, aiguë, hantait toutes mes journées. Elle me semblait justifiée, mais c'est sans doute la paranoïa elle-même qui me donnait cette impression. Dans le cadre de mes recherches sur Anonymous, je devais impérativement veiller à ce que la police ne s'approche pas de moi et, surtout, de mes données. Franchir une frontière exigeait des préparatifs de plusieurs jours où je sécurisais mes notes et configurais un ordinateur spécialement pour le voyage. La menace d'un interrogatoire me semblait toujours imminente; la question n'était pas de savoir *si* les agents du renseignement allaient me contacter, mais *quand* ils le feraient. Je devais protéger mes sources avec vigilance. Je rappelais aux membres d'Anonymous l'importance de faire attention à ce qu'ils me révélaient. Je ne me branchais jamais aux canaux privés où ils planifiaient leurs opérations illégales.

Quant à l'État, je m'en cachais – au grand jour. Mon existence n'avait rien d'anonyme. Là résidait toute l'ironie de la chose: je donnais des conférences sur Anonymous, j'avais été interviewée par 150 journalistes et je discutais régulièrement du collectif à la radio et à la télévision.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Professeure dans une université réputée, j'étais facile à trouver. Les cadres supérieurs d'une des plus puissantes sociétés du monde m'ont même contactée personnellement dans l'espoir d'en apprendre un peu sur une entité que nombre d'entre eux commençaient à craindre.

Pendant des années, j'ai été hantée par un cauchemar récurrent. Des agents du renseignement cognaient à ma porte. Je bondissais du lit en sursaut, le cœur battant: «Ça y est. Ils sont là.» C'était comme dans *Poltergeist*, sauf que le lit ne tremblait pas et que mon impression d'être possédée du démon s'évanouissait dès que je me redressais dans le lit.

*
* *

Par un matin du printemps 2012, je dissipe les traces d'un sommeil tourmenté avec un café bien tassé, laissant le cauchemar derrière moi pour une autre journée. Ma lucidité retrouvée, je réalise que, en ce 19 avril, les rôles seront inversés: aujourd'hui, c'est moi qui vais frapper à la porte du Service canadien du renseignement de sécurité (SCRS), l'équivalent canadien de la Central Intelligence Agency (CIA). Animée d'un sentiment combinant appréhension, ambivalence et surtout curiosité, j'ai accepté l'invitation du service à présenter un exposé sur Anonymous. J'y vais dans le but de savoir ce que le renseignement canadien pense du collectif: le perçoit-on comme une menace terroriste, comme une bande d'activistes turbulents et enragés ou comme toute autre chose? Mon intention cachée consiste à tester sa réaction au *lulz*: une agence traitant de questions de sécurité nationale est-elle en mesure de saisir l'humour propre à Anonymous? Pour le savoir, j'ai concocté un petit test sur le *lulz*.

Les bureaux du SCRS sont situés en banlieue d'Ottawa, dans un immeuble anonyme gris-bleuté. Je m'y rends seule, en taxi, hantée par la pensée d'Orwell, de *Brazil*, de Huxley, de Kafka, et de la surveillance totale mise en place sous Bush et Obama. Des questions fusent dans ma tête. *Qu'est-ce que je fais ici? Qu'est-ce qui se cache dans l'ombre, derrière les murs de l'agence d'espionnage du Canada? La réalité est-elle aussi*

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

terrifiante que je l'imagine? Y a-t-il des salles de surveillance high-tech comme dans Minority Report*? Y mène-t-on des expériences psychologiques dans des salles d'interrogatoire stérilisées aux murs en acier?*

En replaçant mon tailleur mal ajusté, j'essaie de me convaincre que l'immeuble n'abrite qu'une suite de cubicules ennuyeux où l'on remue de la paperasse et tient des réunions dans de mornes salles aux tables pourvues de téléphones à haut-parleur. Peut-être y a-t-il sur le réfrigérateur de la salle de repos une note passive-agressive destinée à la personne qui a mangé tous les Timbits prévus pour un pot de départ en fin de journée. Peut-être y a-t-il au-dessus du lavabo un post-it taché disant: «Ta mère ne travaille pas ici, alors tu devras laver ta vaisselle.» *Ça va aller*, me dis-je.

Pour atténuer mon anxiété, je me suis promis de ne rien dire de nouveau ou de secret, de m'en tenir à des informations déjà accessibles au public et de faire don de mes modestes honoraires à un groupe de défense des libertés civiles. Mais en franchissant le seuil, même si j'ai déjà prononcé cette conférence des dizaines de fois, je me sens plus petite que mon modeste mètre cinquante. Une femme en tailleur m'accueille. Tout me semble bien ordinaire; rien de menaçant en vue, seulement quelques plantes vertes sans intérêt.

Sans attendre, on m'emmène dans une salle équipée d'une petite scène. L'atmosphère est tendue. Je n'arrive pas à discerner l'expression du visage des personnes présentes. Je suis presque paralysée d'appréhension. Je crains soudain que ma nervosité me fasse dire des choses que j'aurais préféré taire. Après tout, ces agents sont formidablement entraînés à l'art de soutirer des renseignements; ils savent tirer parti de toute faiblesse, saisir toute occasion de prendre l'avantage. Plus de 40 personnes ont les yeux braqués sur moi; le sérieux de l'ambiance me transperce. Malgré cela, j'ai donné cette conférence tant de fois que je peux me mettre en pilote automatique. C'est donc au moins dix minutes après avoir commencé que je réalise que mes mains tremblent sensiblement, alors que je tente d'appuyer sur une touche de mon ordinateur en vue de procéder à mon test. Celui-ci consiste à présenter la vidéo virale qui a enflammé l'esprit révolutionnaire d'Anonymous. Chaque fois que j'ai montré cet extrait, trois phrases ont

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

invariablement provoqué l'hilarité générale. Le *lulz* suscitera-t-il le *lol* chez les employés du SCRS? Alors que des nuages s'amoncellent rapidement au-dessus d'un immeuble de verre on ne peut plus banal, une voix proclame, sur un ton dramatique: «Anonymous en est venu à la conclusion que votre organisation mérite d'être détruite. Pour le bien de vos fidèles, pour le bien de l'humanité – et pour notre plus grand plaisir. Nous allons vous expulser d'internet et procéder au démantèlement de l'Église de scientologie sous sa forme actuelle.»

La salle explose de rire. Mission accomplie: rien n'aurait pu mieux démontrer le caractère contagieux de l'esprit du *lulz*. Des agents du renseignement s'esclaffent devant une vidéo empreinte de *lulz* créée par les trolls d'Anonymous à l'origine de la «menace» qu'on les a chargés d'évaluer. *Finalement, je vais m'en sortir vivante*, me dis-je.

La conférence terminée, j'accompagne une partie du groupe dans une salle exiguë, défraîchie et sans fenêtres où, à la lueur de lampes fluorescentes, nous avalons des sandwichs insipides et des cookies. Je me demande si l'immeuble comporte une salle de conférence plus jolie, munie de grandes fenêtres, qui serait réservée aux politologues, aux économistes et à d'autres invités plus prestigieux. Nous prenons place sur des chaises de bureau et faisons un tour de table pour nous présenter. Je suis encore un peu trop perturbée pour retenir les titres et les fonctions de tout le monde, et encore moins leurs noms. Je ne vais certainement pas prendre de notes ou enregistrer la conversation, mais je soupçonne que mes hôtes, eux, le font. Pour ce que j'en sais, je pourrais tout aussi bien être en train de discuter avec des concierges qu'avec des employés disposant du plus haut niveau d'habilitation en sécurité. Un titre retient cependant mon attention: celui de l'autre anthropologue se trouvant dans la salle. En se présentant, il me fait signe de la tête et me sourit. De mon côté, je tente de rester impassible. Toutes sortes de questions me taraudent l'esprit. *Possède-t-il vraiment une formation en anthropologie? Dans quelle université a-t-il étudié? Qui était son directeur de thèse? Quand et pourquoi a-t-il décidé de travailler pour le SCRS? Est-il mieux payé qu'il le serait à l'université?* Mais je garde mes interrogations pour moi. Je crains que l'on confonde ma curiosité avec de

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

l’intérêt pour un emploi au SCRS et je souhaite éviter toute proposition de recrutement.

Au fil d’une conversation qui m’a d’abord semblé décousue, je finis par comprendre pourquoi on m’a invitée. Le SCRS veut savoir une seule chose: si je crois qu’Anonymous envisage de s’en prendre au réseau électrique. Le moment n’a pas été choisi au hasard. À peine un mois auparavant, la NSA a déclaré que le collectif constituait une menace imminente à la sécurité nationale; j’imagine que le Canada a été amené à s’intéresser de plus près à ce groupe énigmatique sous la pression de son voisin du Sud.

Je réponds avec franchise. Quelles qu’aient été ses méthodes, légales ou illégales, Anonymous n’a jamais publiquement appelé à de telles attaques. Pour le moment, rien ne permet de croire que le collectif puisse même l’envisager. En donnant cette réponse au SCRS, je n’ai pas l’impression de révéler un secret, car j’ai déjà expliqué la même chose aux médias. En fait, je crois plutôt rendre service à Anonymous.

Professeure très occupée, je ne peux évidemment pas passer tout mon temps sur les nombreux canaux des divers réseaux IRC, et encore moins surveiller chaque salon de discussion où de telles considérations pourraient être échangées. Sans parler des conversations privées et des canaux sur invitation auxquels je ne me suis jamais branchée. «Leur sociologie est un labyrinthe», dis-je à mes hôtes. Laissant peut-être voir les frustrations que j’ai ressenties en menant mes recherches, j’explique posément ma démarche à mes interlocuteurs. J’ai probablement passé plus de temps devant mon écran d’ordinateur à chatter avec des membres d’Anonymous que toute autre personne étrangère au collectif, à part peut-être les informateurs, forcés de rester en ligne presque à temps plein, et je n’ai jamais perçu le moindre indice de l’existence d’un tel plan. D’ailleurs, le moindre projet d’action radicale, y compris la divulgation de données privées touchant des policiers hostiles, suscite de houleux débats moraux. «Même si Anonymous agit souvent de façon sournoise et diablement déroutante, les Anons n’ont certainement pas l’intention de tuer qui que ce soit. Ils s’organisent à domicile, où, sans doute en petite tenue, ils pianotent sur le clavier comme

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

des forcenés. La seule “violence” à laquelle ils peuvent s’adonner est virtuelle: c’est celle des batailles qu’ils mènent dans *World of Warcraft*, un jeu vidéo très populaire chez eux.» Je conclus mon exposé sur une touche d’humour en citant une blague lancée par un Anon après que la NSA eut affirmé que le collectif était en mesure de s’attaquer au réseau électrique: «C’est vrai. Nous allons bel et bien foutre en l’air le réseau électrique. Nous saurons que nous avons réussi quand tout l’équipement dont nous avons eu besoin pour organiser la campagne sera devenu complètement inutilisable.»

Les postures se décontractent aussitôt. Le rire se fait de nouveau entendre chez les espions canadiens. J’ai vraiment l’impression que mon témoignage les a soulagés. Ils peuvent maintenant retourner à des affaires plus pressantes.

La blague a ouvert la porte à d’autres échanges, qui portent cette fois sur le rôle central des médias dans l’amplification du pouvoir d’Anonymous. Un agent du SCRS reproche amèrement à la presse d’avoir rendu ce collectif de collectifs plus puissant qu’il n’aurait dû le devenir. Essentiellement opposés l’un à l’autre, le service de renseignement et Anonymous se révèlent néanmoins solidaires (quoique très mollement) dans leur ambivalence vis-à-vis des médias de masse, ce qui m’enchante, je dois l’admettre. Tout le monde s’entend sur le fait que les médias ont contribué à faire du collectif ce qu’il est aujourd’hui.

L’anthropologue en résidence du SCRS, un spécialiste du terrorisme au Moyen-Orient, lance alors un commentaire qui parvient à m’ébranler: les djihadistes, m’apprend-il, sont impressionnés par l’ampleur de l’attention médiatique obtenue par Anonymous. *Ai-je bien entendu?* Je n’arrive pas à me figurer des agents d’Al-Qaïda en train de regarder des vidéos du collectif. Et je n’arrive pas plus à concevoir qu’ils puissent en saisir la culture et la pensée politique, en particulier le *lulz*. Je les imagine plutôt rebutés par les pratiques profanes, infidèles et offensantes d’Anonymous. Riant de bon cœur, nous affirmons de concert qu’il est peu probable que les terroristes djihadistes chantent les louanges du *lulz* (dont ils sont sans doute complètement dépourvus). La conversation me rappelle ces propos tenus par un Anon lors d’une séance de chat informelle:

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> <A> oui, c'est l'idée de l'humour et de l'irrévérence qui est au cœur de tout ça [Anonymous]
> <A> c'est ce qui fait qu'on ne pourra jamais l'étiqueter comme terroriste

Malgré la rigolade, je me sens encore assez mal à l'aise, très consciente de mon masque de professeure flegmatique. J'ai l'air calme et posé, mais, dans les faits, je suis troublée. *Je n'arrive pas à croire que je suis en train de faire des blagues sur les djihadistes, Anonymous et le* lulz *avec le SCRS!* Je ne demanderais pas mieux que de m'en aller, ce que je finirai par faire une fois le repas terminé. Rentrée à l'hôtel, je me sens soulagée. Une pensée m'envahit cependant, que je tente de chasser: retenue par le SCRS, ma chambre de l'hôtel Lord Elgin, au centre-ville d'Ottawa, serait-elle truffée de micros?

Encore aujourd'hui, je doute de mon choix d'avoir accepté l'invitation du SCRS. Dans de telles situations, il arrive qu'on divulgue sans le vouloir des renseignements importants, même si les agents ne demandent ou ne cherchent rien de particulier. Peut-être était-il contraire à l'éthique de souligner le rôle joué par les médias dans l'amplification du pouvoir d'Anonymous, un peu comme si j'avais levé le rideau pour révéler que le magicien n'est qu'un petit vieillard aux commandes d'une machine. En revanche, la question du rôle des médias est un secret de Polichinelle au sein d'Anonymous, un sujet dont les militants eux-mêmes discutent régulièrement.

Avec le recul, je crois que, pour le meilleur et pour le pire, c'est l'esprit *trickster* d'Anonymous qui m'a poussée à me rendre aux bureaux du SCRS. À l'instar du dieu nordique Loki, les *tricksters* maîtrisent mal leurs impulsions, motivés qu'ils sont par le désir ou la curiosité. En dépit de mon anxiété et de mes réserves, j'ai rendu visite aux agents du renseignement parce que j'étais intriguée. Une question brûlante me titillait: le *lulz* les ferait-il rire? J'imagine que, comme les trolls, «je l'ai fait pour le *lulz*». Grâce à mon incursion chez les espions canadiens, j'ai obtenu ma réponse: tout le monde (ou presque) peut apprécier le *lulz*. Mais j'ai appris autre

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

chose encore, cette fois grâce à l'anthropologue avec qui j'ai blagué sur les djihadistes et le *lulz*. Il s'agit d'une leçon importante, que je me dois de partager avant que nous n'entreprenions l'aventure que constitue ce livre.

Aucun groupe ou individu ne dispose d'un droit de propriété sur le nom «Anonymous», et encore moins sur son iconographie. Naturellement, cela a aidé Anonymous à se répandre aux quatre coins du globe. Ce nom est devenu la marque antimarque par excellence. Se manifestant sous diverses formes, prenant différentes significations, il est aussi devenu le visage populaire de l'agitation en maints endroits du monde. «Anonymous» peut donc être utilisé librement par quiconque. Malgré cela, comme le rappelle l'exemple des djihadistes, l'ouverture d'esprit radicale propre à l'appellation fait en sorte que tout le monde ne peut pas pour autant (ni ne veut) l'adopter ou se parer de l'iconographie qui l'accompagne. La culture se manifeste de drôles de façons, même au sein d'un groupe d'activistes qui, tout en cherchant à repousser les limites, ont créé un des fronts les plus accessibles, les plus résistants et les plus ouverts de la contestation contemporaine.

Au moment de ma visite au SCRS en 2012, Anonymous était déjà devenu un collectif tentaculaire, prolifique et imprévisible. Évidemment, parce que le groupe est né sur internet, ses mobilisations les plus vigoureuses et les plus populaires visent à défendre les valeurs associées à cette plateforme, telle la liberté d'expression. «La liberté d'expression n'est pas négociable», a lancé un de ses membres. Néanmoins, les Anons ont montré à maintes reprises que leurs préoccupations ne se limitent pas aux libertés civiles. Ces dernières années, ils ont contribué à des campagnes très variées, allant de la dénonciation de viols (notamment à Halifax et à Steubenville) au soutien actif des militants du Printemps arabe de 2011.

Divers facteurs contribuent au maintien de la flexibilité d'Anonymous. Ses membres n'ont pas à remplir de mandats définis d'un commun accord. Ils résistent farouchement à l'institutionnalisation du collectif, dont la réputation est difficile à souiller. Il n'est même pas nécessaire d'être un hacker (si, si!) pour participer à une opération. Avec ses accents hollywoodiens, l'esthétique clinquante d'Anonymous fait vibrer une corde

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

sensible dans la société du spectacle. Enfin, le collectif réagit aux événements mondiaux par une vaste gamme d'actions, dont les plus retentissantes sont la divulgation de renseignements et la révélation de failles de sécurité.

En raison de tous ces facteurs (qui se combinent dans diverses proportions et sous diverses formes), il est pratiquement impossible de connaître à l'avance le moment et les motifs de la prochaine action d'Anonymous, pas plus qu'on ne peut prédire l'apparition d'un nouveau nœud, le succès d'une campagne et un changement d'orientation ou de stratégie en cours d'opération. C'est sans doute en raison de son comportement imprévisible qu'Anonymous fait si peur aux gouvernements et aux entreprises du monde entier.

Même si Anonymous s'est avéré très difficile à étudier, sa conduite n'est ni complètement aléatoire ni simplement chaotique. Être un Anon implique d'adhérer à un ensemble de principes connexes. Animé d'un esprit de déviance humoristique, le collectif utilise un certain nombre de dispositifs techniques (dont l'IRC), refuse la culture de la célébrité et mène des interventions politiques incroyablement riches et variées. Ce livre a pour but de démêler certains aspects complexes et paradoxaux de cet acteur politique qu'est devenu Anonymous. Mais, avant de nous pencher sur ses actions militantes, portons un regard attentif sur l'univers sinistre des trolls, au sein duquel est né le collectif.

---

[*] Les mots suivis d'un astérisque renvoient au glossaire en fin d'ouvrage. [NdÉ]

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Chapitre 1

Trolls, *tricksters* et *lulz*

AVANT 2008, C'EST-À-DIRE avant l'émergence soudaine d'une sensibilité militante chez les membres d'Anonymous, ce nom était exclusivement associé à ce que, dans le jargon d'internet, on appelle le *trolling*, ou trollage, une pratique consistant à salir la réputation de personnes ou d'organisations en répandant des informations humiliantes à leur endroit. Rendu célèbre par ses campagnes de trollage de masse, le collectif était cependant loin d'occuper ce terrain seul: l'univers des trolls était alors vaste et diversifié (et l'est encore aujourd'hui). Activité polymorphe très répandue en ligne, le trollage est pratiqué par une myriade d'associations très unies (dont Patriotic Nigras, Bantown, Team Roomba et Rustle League); il prend diverses formes (qui se distinguent essentiellement par le choix de leurs cibles; par exemple, les *griefers** s'attaquent aux *gamers**, les *RIP trolls* ciblent les proches de personnes récemment décédées) et possède son propre petit panthéon (où trônent violentacrez[1] et Jameth). Son origine remonte à bien avant les balbutiements d'internet, dans les aléas du mythe et de la tradition orale. Malgré leur diversité, les trolls qui sévissent aujourd'hui sur internet affirment de façon quasi unanime que le *lulz* est à la fois la force motrice et l'effet désiré de leurs interventions. Nous amorcerons donc notre tour d'horizon avec le portrait d'un troll parmi les plus tristement célèbres.

*

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

* *

Le 28 août 2010, je constate que j'ai reçu un coup de fil. Surgissant de nulle part, Andrew Auernheimer, un des trolls les plus célèbres de tous les temps, essentiellement connu sous le pseudo de weev, a laissé un message de soixante secondes sur ma boîte vocale:

> Oui, Mme Coleman. C'est weev. W-E-E-V. J'imagine que vous connaissez mon travail. On m'a dit que vous présentiez un exposé sur les hackers, les trolls et la politique-spectacle. Je veux simplement vous dire que je suis *le* maître du spectacle. C'est mon art, madame. On m'a aussi dit que vous aviez fait un genre de présentation sur le *lulz*; j'étais là quand ce mot a été prononcé pour la première fois. Je veux donc m'assurer que vous interprétez et représentez ma culture et mon monde correctement. Je ne veux pas qu'un genre de charlatan propage des mensonges sur mon histoire et ma culture. C'est pourquoi j'aimerais parler un peu avec vous et comprendre ce que vous faites, pour être certain que vous n'êtes pas une autre de ces universitaires de merde. Alors vous pouvez me joindre par courriel à gluttony@XXX.com: G-L-U-T-T-O-N-Y at X-X-X point com. J'attends votre réponse, Mme Coleman. C'est *extrêmement* important.

Le message me frappe tellement que je laisse tomber le téléphone. Je suis submergée par l'exaltation. Mais aussi par la peur. Je ramasse l'appareil, compose la suite de chiffres qui cette fois me semble interminable, puis écoute le message trois fois de suite avant de le sauvegarder. Je rentre à la maison au pas de course, où je passe la soirée à me ronger les sangs: j'aurais en fait préféré qu'il n'ait jamais appelé.

La réputation de weev le précède. Jusque-là, dans le cadre de mon survol de l'univers des trolls et de ma recherche sur Anonymous, je l'ai évité comme la peste. Bien que le trollage soit souvent vécu et présenté comme un jeu, il a une aura de mystère et de danger. weev est l'ancien président d'une des cliques de trolls les plus fermées qui existent encore aujourd'hui, au nom plutôt choquant de Gay Niggers Association of

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

America (GNAA, association des Nègres gays des États-Unis). (Ses membres testent les recrues potentielles sur leur connaissance d'un obscur film de science-fiction de série B intitulé *Gayniggers from Outer Space*, qui a inspiré le nom du groupe.) Entrer en contact avec un troll si abject pourrait être source d'ennuis. Les trolls sont réputés pour leurs campagnes destinées à «ruiner une vie», comme ils disent, lors desquelles ils font circuler des rumeurs avilissantes (fondées ou non) sur quelqu'un et divulguent des renseignements cruciaux tels que son adresse et son numéro de sécurité sociale. La victime se sent à la fois maudite, étiquetée et stigmatisée; elle peut souffrir de séquelles psychologiques pendant longtemps[2].

Mais, parce qu'il serait également risqué d'ignorer la requête de weev (qu'il a tout de même qualifiée d'extrêmement importante), je décide au bout de quelques jours de lui écrire. Et, puisque de toute façon je me jette à l'eau, je me dis que cette rencontre m'offrira l'occasion de me familiariser avec un autre type de troll. Car Anonymous pratique depuis ses débuts un trollage où l'égo s'efface derrière la masse, contrairement au style vantard, élitiste et arrogant de weev. Ils font tous deux partie de la même «tribu», à la manière dont les deux faces d'une même médaille s'opposent l'une à l'autre. Pendant environ deux minutes, l'idée de dresser une typologie exhaustive des trolls me procure un enthousiasme éphémère. À l'instar de mes ancêtres anthropologues qui catégorisaient tribus, crânes et haches, je pourrais classifier les trolls et leurs abominables exploits, et, en cédant au penchant historique de ma discipline pour les catégories sans fondement et parfois racistes, je jouerais ainsi moi-même les trolls. Mais je déchante vite en songeant aux représailles auxquelles je m'exposerais s'il m'arrivait de prendre à rebrousse-poil un de ces trolls de triste renommée. Je me souviens que, si j'ai décidé de concentrer mes recherches sur l'activisme d'Anonymous plutôt que sur l'époque où ses activités de trollage étaient à leur paroxysme, c'est pour une bonne raison. J'en viens donc à espérer que mon envoi à weev reste lettre morte.

Quand arrive sa réponse, je réalise que je n'ai d'autre choix que de respecter mon engagement. Nous finissons par communiquer par la

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

messagerie instantanée de Skype. Il utilise le pseudo de dirk diggler (que l'on pourrait traduire par «bite en forme de poignard»), d'après le nom du personnage de la vedette porno dans le film *Boogie Nights*, sorti en 1997. Plus tard, quand nous passerons à l'Intenet Relay Chat (IRC), il reprendra le nom de weev.

<dirk diggler> comment allez-vous?
<biella> bien et vous?
<dirk diggler> je me remets des effets d'une substance néfaste
<biella> vous vous levez tôt
<dirk diggler> je pense qu'on appelle ça de la méthylènedioxypyrovalérone
<dirk diggler> techniquement, il est tard
<dirk diggler> j'ai pas dormi
<biella> je me suis levée à 3 heures du matin, mais c'est assez banal pour moi
<dirk diggler> je suis en train de travailler sur mes dernières saloperies
<dirk diggler> les progrès technologiques nuisibles vont bon train
<biella> vous êtes assez compétent en la matière
<dirk diggler> oui, je troque la mdpv pour le café
<dirk diggler> j'espère que ça va calmer cette spirale infernale assez longtemps pour que je puisse envoyer cette merde aujourd'hui
<biella> y a-t-il une possibilité que vous alliez à new york bientôt?
<dirk diggler> c'est peu probable
<dirk diggler> c'est une ville horrible
<biella> ha ha, vraiment?
<dirk diggler> un endroit répugnant
<biella> pourquoi?
<dirk diggler> à new york, les seules personnes dignes de respect sont les israélites noirs

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<dirk diggler> new york est une ville fondée sur l'ordre répugnant des financiers

Vu la crise que vient de provoquer la négligence de Wall Street, cette dénonciation de l'«ordre répugnant des financiers» a un fond de vérité. C'est ainsi que, quelques minutes à peine après avoir entamé une conversation sincère avec un troll de renommée mondiale, je tombe d'accord avec lui:

<biella> c'est vrai
<dirk diggler> cet endroit est immoral et décadent
<biella> il y a de moins en moins de place pour les non-riches
<dirk diggler> et dès que des individus sans morale ont le pouvoir, je constate que tout le monde essaie de les imiter
<biella> à mon humble avis, detroit est la seule ville où il y a des possibilités (grande ville)
<dirk diggler> non, slab city est l'endroit des états-unis qui a le meilleur potentiel
<dirk diggler> une partie de la guerre de dieu s'y déroule en ce moment
<biella> jamais allée

C'est vrai: je n'ai jamais mis les pieds à Slab City. En fait, je n'en ai jamais entendu parler. Pendant que nous chattions, je google «Slab City», l'endroit existe bel et bien. Il s'agit d'un refuge hivernal pour campeurs et squatteurs du Wild West situé en Californie, dans le désert du Colorado. Je réalise vite que, même s'il ment souvent, weev dit aussi souvent la vérité et qu'il possède des connaissances encyclopédiques en matière d'étrange, de fantastique et de scabreux. Bref, weev est un ethnographe autodidacte des formes les plus extrêmes et abjectes de la marginalité humaine.

En consacrant l'essentiel de sa vie d'adolescent et de jeune adulte au piratage et au trollage – et, selon ses dires, à la consommation de quantités phénoménales de drogue –, weev s'est constitué un vaste catalogue d'exploits techniques et humains. Son coup le plus fameux, qui lui a valu

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

une sentence de trois ans et demi de prison, a frappé la société AT&T, une cible de choix chez les hackers en raison de son empressement cordial à transmettre des informations au gouvernement des États-Unis. (Les pratiques bien connues auxquelles se livrait AT&T dans la salle 641A, un centre d'interception des télécommunications géré par la National Security Agency (NSA), semblent insignifiantes depuis qu'on sait que la plupart des géants des télécommunications et d'internet permettent généreusement aux autorités d'accéder aux données sur leur clientèle.) weev s'en est pris à AT&T avec Goatse Security, un sous-groupe improvisé de la GNAA chargé des questions de sécurité. En juin 2010, ces trolls ont découvert que le géant américain des télécommunications avait fait une erreur stupide et irresponsable: toutes les données recueillies auprès de ses clients utilisateurs d'iPad avaient été stockées sur internet sans protection. Normalement, une firme qui applique des normes de sécurité adéquates crypte les renseignements comme le nom de ses clients, leurs adresses électroniques et le numéro d'identification unique de leurs iPad. Mais, du moins dans ce cas, AT&T n'avait rien crypté du tout.

Certes, les données n'avaient pas été déposées sur le pas de la porte avec une pancarte «Servez-vous». Mais elles étaient étrangement faciles d'accès. Les hackers de Goatse Security ont simplement trouvé une façon de les «aspirer» à l'aide d'un script (petit programme informatique facile à utiliser) écrit par l'un d'eux, Daniel Spitler, connu sous le pseudo de JacksonBrown. Baptisé «iPad 3G Account Slurper» par l'équipe de *gray hats** (chapeaux gris), le script a permis de recueillir les données de 140 000 clients. Ce genre d'occasion – celle de mettre au jour une faille de sécurité d'une telle ampleur – est irrésistible pour un hacker, même pour un type comme weev, qui, comme il me l'expliquera lorsque nous finirons par nous rencontrer en personne, n'est pas aussi ferré en technologie que ses confrères (à moins qu'il ne soit tout simplement trop paresseux pour s'occuper des tâches fastidieuses, car il maîtrise quand même une bonne partie des aspects techniques les plus pointus de la sécurité informatique).

Quoi qu'il en soit, c'est Spitler qui avait programmé le script. Poursuivi en justice, il plaiderait coupable. En novembre 2012, weev serait

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

aussi reconnu coupable d'avoir «piraté» le système d'AT&T, en violation du Computer Fraud and Abuse Act (CFAA, loi sur la fraude et la malveillance informatiques). Néanmoins, un fait demeure: puisque le système était dépourvu de tout dispositif de sécurité, on ne pouvait, techniquement, le «pirater». Le script de Daniel Spitler n'avait pas endommagé le système d'AT&T, dont les autres éléments étaient sécurisés, et weev, qui avait apporté des améliorations mineures au programme, s'était surtout chargé de publiciser l'opération en révélant, sans contrepartie, la faille aux médias. Son objectif consistait à lever le voile, à la fois dans l'intérêt du public et en vue d'asseoir sa réputation, sur la négligence spectaculaire d'AT&T. Il importe de souligner que la CFAA est un outil juridique particulièrement grossier: cette loi ratisse si large qu'elle confère aux autorités judiciaires un pouvoir considérable dans toute poursuite touchant de près ou de loin à la notion plutôt vague d'«accès non autorisé à un ordinateur». Il n'est même pas nécessaire que les faits reprochés relèvent du hacking. Certains tribunaux ont appliqué la notion d'«accès non autorisé» au fait de s'être servi d'un ordinateur en contrevenant simplement aux conditions générales d'utilisation ou à d'autres règles imposées par son propriétaire[3].

Une fois weev condamné, son cas a attiré l'attention d'un trio d'avocats de premier ordre: Orin Kerr, Marcia Hofmann et Tor Ekeland. Dans le but de renverser ce qu'ils considéraient, à l'instar de nombreux experts en sécurité, comme un dangereux précédent capable d'effaroucher des chercheurs en sécurité informatique dont les travaux sont essentiels, ils ont porté le jugement en appel. Pour déceler ses faiblesses et renforcer ses infrastructures (dans son propre intérêt comme dans celui du public), l'industrie de la sécurité dépend de hackers et d'informaticiens qui cherchent des failles en ayant recours aux mêmes méthodes que leurs homologues criminels. Finalement, en avril 2014, après que weev eut purgé environ douze des quarante-et-un mois de sa peine, le jugement a été annulé. L'annulation n'est pas imputable aux arguments avancés par la partie appelante à propos de la CFAA, mais plutôt à l'endroit où s'est tenu le procès initial. La Cour d'appel a établi que le crime n'avait pas été

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

commis dans le New Jersey, l'État où le procès s'est déroulé. Tor Ekeland a expliqué l'importance de cette décision au *Guardian*: «Si la Cour d'appel avait tranché dans l'autre sens, la notion d'instance universelle se serait désormais appliquée [...] aux cas de fraude et de malveillance informatiques, ce qui aurait eu des conséquences très importantes sur internet et le droit informatique[4].» Néanmoins, même s'ils ont été enchantés d'apprendre qu'on l'avait libéré et qu'on avait éclairci les questions relatives à l'endroit où se déroule un procès, les défenseurs de weev sont nombreux à déplorer que la Cour ait évacué le problème plus global de la constitutionnalité de la CFAA, qui demeure entier.

En transmettant l'information aux médias, weev a montré que ses intentions allaient au-delà du simple trollage. Tout hacker qui se respecte se scandalisera d'une sécurité informatique déficiente; en parler à la presse, capable d'en faire toute une histoire, peut donc s'avérer un choix responsable. Évidemment, comme je le constaterai en l'écoutant me raconter son histoire, weev a aussi agi pour le *lulz.* La moindre mention de Goatse Security dans la presse le fait pouffer de rire. Il imagine ces millions de personnes qui, ayant googlé l'étrange nom du sous-groupe de la GNAA chargé des questions de sécurité, ont un haut-le-cœur à la vue de l'abjecte «supernova anale» qui rayonne sur leur écran[5]. *Goatse* est en fait une image grotesque, amplement reproduite sur internet, où l'on voit un homme penché en avant qui s'écarte les fesses plus largement qu'on le croirait humainement possible. Incapables de faire comme s'ils ne l'avaient jamais vue, ceux qui y ont été exposés en retiennent le moindre détail, ont l'esprit marqué au fer rouge par ce cul béant. Au souvenir de cette blague puérile, weev en vient à rire aux larmes; les yeux plissés, plié en deux, il se tient les côtes et secoue ses épaules comme un marteau-piqueur démoniaque.

Il est indéniable que weev a choqué tout le monde, y compris les autorités judiciaires. Rien sans doute ne pourrait mieux témoigner de son insolence que la sévérité de la peine qu'on lui a infligée. Après tout, il n'avait même pas participé à la programmation du script. La veille du prononcé de la sentence, il écrivait sur Reddit, un site de partage de liens populaire chez les nerds*: «Mon seul regret est d'avoir été assez gentil pour

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

laisser à AT&T le temps d'apporter des correctifs avant de transmettre les données à *Gawker*. Je ne serai pas aussi généreux la prochaine fois[6].» Pour justifier la sentence, la poursuite ne s'est pas contentée de citer ce commentaire une seule fois, ni deux: elle l'a cité trois fois!

De la part de weev, des propos incendiaires comme ceux-là n'ont rien d'exceptionnel. Il a même enregistré et posté sur YouTube des discours haineux à l'endroit des Juifs et des Afro-Américains. Ces «sermons», comme il les appelle, sont si hargneux qu'ils dégoûtent même les autres trolls.

Quand nous amorçons notre échange, les ennuis judiciaires de weev avec AT&T viennent tout juste de commencer. Au cours des cinq mois qui suivront, nous discuterons beaucoup. Certains de nos échanges seront particulièrement bizarres. Prenons par exemple cette conversation de décembre 2010:

<weev> salut
<weev> comment ça va
<biella> bien et vous?
<weev> peux pas me plaindre
<weev> la GNAA a changé de mode de gouvernance
<weev> c'est maintenant une démocratie athénienne
<weev> où ceux qui ont accompli leur service militaire
<weev> i.e. fait du trollage sympa
<weev> ont maintenant le droit de voter sur les mesures

Je suis incrédule. Mais j'arrive – non sans peine – à taper une réponse:

<biella> vraiment?

Puis, sans crier gare, comme c'est souvent le cas en situation de chat – en particulier avec weev –, mon interlocuteur change de sujet pendant que je suis en train de répondre à des questions sur la gouvernance.

<weev> mon répondant m'a contacté sans raison

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<biella> comment c'était avant? [avant de devenir une démocratie athénienne]
<weev> oui
<weev> je pense qu'on va m'arrêter demain ou le 16
<weev> je dois répartir les responsabilités
<weev> parce que personne pourrait faire toute la merde que j'ai faite
<biella> vraiment? [...]
<biella> je veux dire, pourquoi croyez-vous qu'on va vous arrêter?
<weev> mon garant m'a contacté sans raison
<weev> pour savoir où je suis
<weev> la dernière fois que c'est arrivé
<weev> on a défoncé ma porte le lendemain

Au moment où cette conversation a lieu, weev fait l'objet d'une enquête. Je sais qu'il est un troll et tout le reste, mais la prison, admettons-le, c'est moche. Je lui exprime ma sympathie et m'engage à lui rendre visite:

<weev> merci
<weev> je vais apprécier votre compagnie
<biella> et les friandises sans gluten que je vais vous apporter
<weev>:-D
<weev> je viens de découvrir
<weev> comment faire un pain sans gluten passable
<weev> t'as juste à utiliser plein de trucs différents
<weev> de la farine de riz complet, de tapioca et de teff
<weev> et de la fécule de pomme de terre

Cet échange entre un troll sans gluten et une anthropologue sans gluten glisse alors tout naturellement vers le Pilates. Je regrette de ne pas avoir obtenu de réponse satisfaisante au sujet du mode de gouvernance des trolls. Nos conversations prennent souvent une tournure imprévisible et divertissante comme celle-là.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Je garde mon sérieux la plupart du temps, mais j'entre tout de même dans son jeu de faussaire* autoproclamé. Cependant, il m'arrive d'être incapable de résister à l'envie de critiquer ses conneries, et même de le troller un petit peu:

<weev> je connais beaucoup de choses pour un cancre
<biella> sauf que vous avez étudié l'anthropo à james madison:-)
<weev> oui
<biella> mais vous connaissez effectivement beaucoup de choses
<weev> je suis qu'un pauvre plouc de l'arkansas
<weev> j'ai lâché les cours parce c'en était trop pour ma petite tête de gars du sud
<weev> et la dégénérescence des institutions américaines me dégoûtait
<weev> toutes les sciences sociales sont devenues une machination sophistiquée visant à donner un complexe d'infériorité raciale aux jeunes blancs ou à détruire les rôles de genre qui font fonctionner notre société

En tant que professeure de sciences sociales, je connais cette «machination sophistiquée» de l'intérieur. Je ne peux m'empêcher de lui mentir un peu:

<biella> tellement
<weev> ou à promouvoir des idéologues judéo-bolchévo-marxistes
<biella> ils nous forment secrètement à ça (et de façon assez intensive)
<weev> je sais pas si vous êtes sarcastique ou sincère
<weev> c'est ça qui est drôle
<biella> lol
<biella> bienvenue dans le monde de biella qui chatte avec weev:-)

weev sera incarcéré dans plusieurs États américains avant de finir dans une prison du New Jersey, d'où il sera libéré sous caution le 28 février 2011

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

dans l'attente de son procès. Comme il n'est plus autorisé à surfer sur internet, nos séances de chat ont pris fin. Nous poursuivons donc nos conversations en personne, à New York, devant des repas sans gluten. Je prends l'addition, car il est complètement fauché. Il m'apprend beaucoup de choses sur le trollage, mais je ne ferai jamais les frais de son savoir-faire.

Malgré des conditions de libération sous caution lui interdisant d'utiliser un ordinateur, weev parvient encore à exercer son art. Comme bien d'autres trolls, il aime duper les gens dans le but de se faire remarquer. Se placer sous les feux de la rampe procure une sensation extraordinaire, en particulier si l'on n'est pas obligé de payer un spécialiste des relations publiques pour diffuser une fausse *sextape*. En mai 2011, alors que l'été s'installe enfin à New York, je reçois un texto enthousiaste de weev. «Google mon nom», écrit-il. Je m'exécute aussitôt, et des centaines d'articles apparaissent. Je constate que mon troll a leurré les médias en montant un canular sur lui-même, dans lequel il prétendait être le voisin de Dominique Strauss-Kahn alors que ce riche homme politique français et ex-directeur du Fonds monétaire international (FMI) venait d'être accusé de viol. Sans ressources, weev est néanmoins parvenu à transmettre ses commentaires à des centaines de médias. Aucun journaliste ne s'est donné la peine de vérifier ses allégations: «Contrairement à ce qu'affirme le procureur, Strauss-Kahn a déjà rencontré ses voisins. Un hacker tristement célèbre qui vit dans l'immeuble de Broadway soutient avoir fait connaissance avec le Français, qu'il décrit comme "un type bien". "C'est comme un gros *Breakfast Club*, ici", aurait déclaré Andrew Auernheimer, 26 ans, en référence à ce film classique de 1985 où cinq étudiants passent un samedi en retenue, enfermés[7].»

In Lulz We Trust

Si, comme le font tant de trolls, weev agit en mélangeant vérités et mensonges, peut-on attester qu'il se trouvait bel et bien là où le mot «*lulz*» a été prononcé pour la première fois? Pour éclaircir cette question, on peut se

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

tourner vers l'*Encyclopedia Dramatica*, un glossaire en ligne incroyablement détaillé de l'univers des trolls où sont répertoriées leurs méthodes, leur histoire, leurs obscénités et leurs traditions. Malgré son appellation d'«encyclopédie», ce site ne prétend ni à la neutralité ni à l'objectivité. L'*Encyclopedia Dramatica* est certes encyclopédique par son souci du détail, mais elle est également outrageante par son ton et truffée de faussetés. Elle parvient cependant à bien exposer la dynamique morale du trollage (ce qui, étrangement, lui confère une certaine objectivité). Son étymologie du *lulz* (dont voici un extrait) relève-t-elle des faits ou de l'affabulation?

> est une altération de *lol*, acronyme de *laugh out loud* [en français: mort de rire, mdr], et désigne le fait de rire aux dépens de quelqu'un. Ce qui le rend intrinsèquement supérieur aux formes inférieures d'humour. Anonymous se gave de *lulz* en faisant des sales coups au hasard. Ces derniers sont toujours rendus publics sur le net. De la même façon qu'un élément de surprise fait de l'acte d'amour physique un moment merveilleux, l'angoisse d'une victime dont on se moque transforme le *lol* en *lulz* en rendant celui-ci plus long, plus intense et plus agréable. Le *lulz* est pratiqué par des internautes qui ont été témoins de trop de catastrophes économiques, environnementales et politiques, et qui, vu l'état apocalyptique du monde actuel, jugent qu'il vaut mieux entretenir un état de sociopathie volontaire et joyeuse que d'être continuellement *emo*.
>
> Formulé pour la première fois par Jameth, un des premiers administrateurs de l'*Encyclopedia Dramatica*, le terme *lulz* est devenu très populaire sur ce site. Le pseudo de Jameth trouve son origine quelque part en 2001, alors que James (son vrai nom, le suffixe *-th* étant un jeu de mots sur son homosexualité et sa petite 8i73 [bite, en *leet speak**]) discutait avec un homosexuel zézayant. James a été appelé Jameth en raison du défaut de langage de cette personne. En juin 2001, il a décidé d'utiliser Jameth comme nom d'usager sur son

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> compte LiveJournal. Ne le laissez pas vous berner: James a toujours très envie d'une bite[8].

Selon les informations obtenues de diverses interviews, dont une avec le brillant fondateur d'*Encyclopedia Dramatica*, Sherrod DeGrippo, weev a bel et bien participé à la conférence téléphonique où Jameth a introduit le terme *lulz*, et Jameth est bel et bien gay. Je n'ai pas approfondi la question du zézaiement[9].

Aujourd'hui, le *lulz* peut aussi s'appliquer à des plaisanteries légères; il est utilisé et apprécié par des nerds d'internet dans le monde entier. Mais il a d'abord été conçu pour désigner une attitude cruelle, le fait de «rire d'une personne en vue de lui nuire», comme les trolls se plaisent à le définir. Le *lulz* est un terme typique de ce que les folkloristes qualifient d'argot, à savoir un vocabulaire spécialisé et ésotérique en usage au sein d'une sous-culture. De par son opacité et sa spécificité, l'argot favorise la culture du secret ou, à tout le moins, le maintien de cloisons sociales rigides. Pour un anthropologue, il est tentant d'envisager le *lulz* du point de vue de l'épistémologie, de la production sociale du savoir, peu importe à quel point cela peut sembler ridicule. Sous un certain angle, le *lulz* joue le rôle d'un objet épistémique: en cristallisant un ensemble d'expériences, il fait en sorte que celles-ci peuvent devenir matière à réflexion. Pendant des décennies, aucun vocable ne désignait la notion correspondant au *lulz*, ce qui n'empêchait pas les hackers de goûter aux plaisirs particuliers de la facétie. Quand un terme fait son apparition, il ouvre la pratique même qu'il désigne à une réflexion plus poussée de la part des gens qui s'y adonnent. Les trolls d'aujourd'hui pontifient sur la signification du terme, l'appliquent à des actes particulièrement satisfaisants (qu'ils soient accomplis ou non pour le *lulz*) et s'en servent pour diagnostiquer des situations où le *lulz* fait défaut – et qui, bien entendu, demandent l'adoption de mesures correctives.

Mais qu'est-ce que ce terme peut bien signifier qu'on ne pourrait exprimer par un autre mot? La réponse ne va pas de soi. Néanmoins, si l'on garde à l'esprit que *lulz* est un dérivé de *lol*, on constate plus facilement qu'il relève avant tout de l'humour. Quiconque a déjà partagé une blague

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

par courriel connaît bien la signification de *lol* ou de mdr. Le *lulz*, lui, est plus sombre: il se manifeste le plus souvent aux dépens d'autrui, tend à donner des résultats imprévus et frise parfois les propos offensants ou haineux (voire franchit carrément les limites de la décence, comme en font foi, bien sûr, les blagues sur le viol). Indéniablement sulfureux, le *lulz* traduit avant tout l'euphorie de la transgression.

On peut reconnaître les traits distinctifs du *lulz* dans les tribulations de weev avec AT&T: non pas dans sa révélation de la faille de sécurité, mais dans la façon dont il a amené de respectables présentateurs de journaux télévisés de partout aux États-Unis à prononcer le mot «Goatse», et donc à faire référence sans le savoir à une des images les plus répugnantes qu'on puisse trouver sur internet. Concrètement, les activités associées au *lulz* transgressent les limites, mais, ce faisant, elles se trouvent aussi à les confirmer. Un fossé sépare les internautes qui ne pratiquent que le *lol* (sans bien connaître internet, son histoire et son fonctionnement) de ceux qui ont adopté le *lulz* (les hackers, les trolls et leurs semblables), très au fait des bas-fonds du réseau. Le *lulz* est à la fois un outil de différenciation culturelle et une arme utilisée pour attaquer, humilier et diffamer les simples «loleurs», qui, souvent, ne se rendent même pas compte que toute une culture se dresse contre eux. En général, le *lulz* relève de la blague d'initiés, mais il y a (souvent) égalité des chances: le rire qu'il induit peut se propager à l'extérieur du monde des trolls, chez les gens ordinaires. Être admis dans l'univers du *lulz* n'exige d'ailleurs qu'un minimum de connaissances. Les loleurs peuvent les acquérir en parcourant des sites fréquentés par les trolls, tels *Encyclopedia Dramatica*, 4chan et Something Awful, qui offrent leur savoir à quiconque s'y intéresse. Lorsqu'ils y goûtent, certains d'entre eux prennent aussitôt leurs jambes à leur cou, tandis que d'autres finissent par constituer la prochaine génération de trolls.

Le *lulz* montre l'aisance et la désinvolture avec lesquelles les trolls peuvent ébranler notre sentiment de sécurité en envahissant des espaces privés et en divulguant des données confidentielles. Leurs cibles se font livrer des dizaines de pizzas impayées ou voient leur numéro de téléphone privé, leur numéro de sécurité sociale, leurs communications personnelles,

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

leur numéro de carte de crédit et le contenu de leur disque dur semés à tout vent. Les trolls adorent désacraliser tout ce qui est un tant soit peu sacré, explique la théoricienne de la culture Whitney Phillips. Non sans perspicacité, celle-ci les qualifie d'«organes de digestion culturelle [qui] fouillent le paysage, en refaçonnent les contenus les plus dérangeants et balancent les monstruosités qui en résultent au visage d'une population qui ne se doute de rien[10]». En résumé, tout renseignement tenu pour personnel, sécurisé ou sacré est une cible de choix, à diffuser de multiples façons. Les actions orientées par le *lulz* rompent le consensus politique, éthique, social et esthétique. Tout apriori sur l'inviolabilité du monde devient une arme; les trolls invalident cet apriori en laissant entrevoir la possibilité qu'ont les geeks de détruire le monde, c'est-à-dire de faire de nous ce que bon leur semble.

J'ai commencé à m'intéresser aux trolls au moment même où certains d'entre eux vivaient une transformation fondamentale, les membres du collectif Anonymous se tournant de plus en plus vers l'activisme. Au vu des bas-fonds sordides que je viens d'évoquer, une telle évolution est plus qu'étonnante. Elle n'est toutefois pas dépourvue de précédents historiques: j'ai constaté chez les trolls un lien avec les *tricksters* de la mythologie. Je suis une anthropologue, après tout, et les *tricksters* font l'objet de cogitations anthropologiques depuis les balbutiements de la discipline.

Trick or Treat[11]

On trouve l'archétype du *trickster* chez toutes sortes de personnages légendaires et dans des mythes parfois délectables. La mythologie grecque et romaine a inscrit certaines de ces figures (dont le mercurial Hermès et le bachique Dionysos) au cœur de la culture occidentale. Dans les folklores ouest-africain et caribéen, ce rôle est dévolu à Anansi, une araignée qui tantôt transmet la connaissance ou la sagesse, tantôt sème le doute ou la confusion. Eshu, esprit des communications, des chemins et des carrefours, est tout aussi ambigu. Connu pour plonger les êtres humains dans des

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

intrigues inextricables qui les forcent à prendre des décisions, il peut se comporter en maître bienveillant ou en agent de destruction. Chez les Autochtones d'Amérique du Nord, le Corbeau provoque le changement par sa propre volonté ou par accident, et le Coyote est une bête égoïste prête à duper tout être humain ou animal pour satisfaire ses appétits. Depuis le Moyen Âge, la conception occidentale du *trickster* a souvent été portée par la littérature. Puck, «cet esprit malicieux et coquin» qui «égare la nuit les voyageurs, en riant de leur peine» dans *Le songe d'une nuit d'été*, n'est pas le pur produit de l'imagination de Shakespeare: le Barde s'est inspiré d'une créature féerique du folklore celte. Plus récemment, le cinéma hollywoodien a produit une version insipide de Loki, ce dieu de la mythologie nordique capable de métamorphose, mais a tout de même réussi à faire ressortir le caractère capricieux et vindicatif du *trickster*.

Tous les *tricksters* partagent certains traits, dont un ardent désir de défier ou de transgresser les règles, les normes et les lois. Souvent incapables de résister à leurs impulsions et d'éprouver du remords, ils sont incapables de la moindre retenue dans leurs propos, souvent outranciers. Certains *tricksters* obéissent à une vocation plus noble, tel Loki, qui travaille parfois pour les dieux (même si, en raison de sa redoutable nature, il leur attire des ennuis). Nombre d'entre eux sont poussés par la curiosité et un appétit vorace. Ils planifient rarement leurs actions, laissant plutôt libre cours à leur spontanéité, ce qui se traduit par une imprévisibilité teintée de ruse. Et bien qu'elle soit souvent la clé de leur succès, leur extravagance peut aussi faire capoter leurs plans[12].

Les histoires de *tricksters* ne sont ni didactiques ni moralisatrices; leur morale se révèle plutôt de façon amusante. Elles peuvent avoir une fonction normative (parents racontant des histoires effrayantes à leurs enfants pour les dissuader de mal se conduire) ou critique (mise à nu des normes permettant leur remise en question). «Pour assurer son enracinement, sa vivacité et sa durabilité», écrit Lewis Hyde, qui a longuement réfléchi à la figure du *trickster*, «toute culture doit faire place à des représentations symboliques dont la fonction consiste à dévoiler et à perturber ses propres fondements[13]».

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Dans cette perspective, on peut aisément qualifier les trolls et Anonymous de *tricksters* contemporains. Provocateurs et saboteurs, ils malmènent les conventions depuis la zone liminale qu'ils occupent. Ils sont bien placés pour transmettre des leçons – quel que soit leur objectif initial. Nul besoin d'accepter – et encore moins d'endosser – leurs actions pour en tirer une valeur positive. À la fois prophètes édifiant le peuple par l'annonce de perspectives libératrices ou terrifiantes et symptômes de problèmes souterrains méritant d'être mis au jour, ils sont perçus tantôt comme des forces bienfaisantes de renouveau, tantôt comme des ombres difformes et trompeuses. Ainsi, le *trickster* offre une heuristique (certainement ni la seule ni la plus importante) permettant de comprendre les origines, les innombrables retentissements et, surtout, le double visage d'entités moralement élastiques comme les trolls et Anonymous.

Avant d'en arriver à Anonymous proprement dit, un bref survol de la riche tradition propre aux trolls et *tricksters* sur internet s'impose. De par sa nature même (un réseau édifié à partir de logiciels), internet offre un cadre idéal, tant pour le jeu que pour la bidouille. Un véritable incubateur à mauvais tours[14]. Les hackers (et à leur suite les trolls) s'adonnent d'ailleurs à de telles pratiques depuis très longtemps. Mais ce n'est que récemment que certaines d'entre elles ont acquis une visibilité qui leur a conféré un statut mythique. L'*Encyclopedia Dramatica* regorge de liens sur l'histoire des mauvais tours (*tricksterdom*) technologiques. L'exploration de cet arbre généalogique permet de mieux comprendre ce qui distingue Anonymous (tant ses trolls que ses activistes) du panthéon plus large des *tricksters* technologiques.

(Brève) histoire naturelle des jeux des *tricksters* sur internet (ou généalogie d'une morale douteuse)

weev est un troll de trolls, ce qui le distingue du lot dans un domaine abritant pourtant une grande diversité.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Les trolls ont pour ancêtres une galerie de personnages bigarrés. Le trollage était répandu dans l'underground hacker des années 1980 et 1990, où des hackers subversifs à la recherche de savoirs interdits exploraient sans permission les ordinateurs d'autrui. Mais ces pionniers étaient eux-mêmes redevables de leur effronterie à leurs prédécesseurs immédiats, les *phreakers* ou *phone freaks**. Mêlant espièglerie à la pratique de la spéléologie technologique, les *phreakers* s'introduisaient illégalement dans le réseau téléphonique en reproduisant les fréquences audio utilisées pour l'acheminement des appels. L'idée était pour eux d'en retirer quelque chose d'instructif, mais aussi, certainement, de se griser de la transgression. Dans les années 1960 et 1970, les *phreakers* utilisaient leur savoir-faire pour converser sur des lignes partagées. Ce type d'activité attirait notamment de jeunes aveugles, à qui les liens tissés avec autrui grâce au téléphone procuraient un sentiment de liberté. Par l'entremise des câbles téléphoniques, des gens d'un peu partout se rencontraient sans se voir pour discuter, papoter, échanger des connaissances techniques ou fomenter des mauvais coups – *beaucoup* de mauvais coups, la plupart impliquant naturellement l'utilisation du téléphone. Bien que ces farces fussent généralement sans malice, certaines d'entre elles prenaient parfois un tour assez terrifiant. Dans son histoire des *phreakers*, l'ingénieur Phil Lapsley raconte un canular tristement célèbre, monté en 1974, où de mauvais plaisants avaient tiré parti d'une faille particulière du système téléphonique pour réacheminer tous les appels destinés aux habitants de Santa Barbara, en Californie, vers un faux service d'urgence où l'on entendait cet avertissement: «Une explosion nucléaire s'est produite à Santa Barbara. Toutes les lignes téléphoniques ont été coupées[15].» Fin connaisseur de ce type d'histoires, weev affectionne particulièrement les canulars téléphoniques et se considère comme un héritier de cette illustre lignée.

La fin de la téléphonie analogique, qui a suivi le démantèlement du monopole de «Ma Bell» (maman Bell, surnom affectueux donné à AT&T), a sonné le glas du *phreaking*. À ce dernier s'est substituée l'exploration des réseaux d'ordinateurs, qui a favorisé l'essor de l'underground hacker jusqu'à son apogée dans les années 1990. Si ces hackers marginaux

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

acquéraient, partageaient et développaient des connaissances techniques (en recherchant des failles de sécurité et en élaborant des curiosités techniques), ils avaient aussi goûté au fruit défendu. Sans surprise, leurs activités eurent tôt fait de déborder d'un cadre strictement technique pour englober la moquerie, le spectacle et la transgression. Leur éthique et leurs idées politiques se distinguèrent rapidement de celles des hackers universitaires du Massachusetts Institute of Technology (MIT), de Carnegie Mellon et de Stanford – ces passionnés d'informatique qui, dans les années 1950 et 1960, restaient debout toute la nuit pour avoir accès à leurs ordinateurs adorés, qu'on réservait pour des usages officiels durant le jour. Bien que ces hackers pionniers, dont l'histoire a été racontée de manière admirable par le journaliste Steven Levy, eussent aussi un penchant pour les canulars, ils étaient plus attachés à des valeurs de transparence et d'accessibilité que leurs successeurs de l'underground[16].

Nombreux étaient les membres de l'underground hacker qui se surpassaient en bouffonneries dans leurs activités. Maîtres de l'espièglerie, ils étaient les joyeux rôdeurs des réseaux informatiques. Certains hackers marginaux étaient cependant plus proches de l'archétype de Loki dans leur façon de hanter les réseaux. Quand j'interroge des hackers qui étaient actifs dans les années 1990 sur leurs activités de trollage, la conversation finit toujours par tomber sur le troll le plus redouté de cette époque: u4ea (prononcer «iouforia», pour *euphoria* [euphorie], un nom à connotation sinistrement similaire à celle de *lulz*). Le règne d'u4ea s'est avéré si terrifiant que, chaque fois que je prononce son nom en présence d'un de ses contemporains, la mine de ce dernier s'assombrit et la conversation prend un tour on ne peut plus sérieux. u4ea, un Canadien, est surtout connu pour avoir été le «fondateur, président et dictateur à vie» d'un groupe de hackers appelé BRoTHeRHooD oF WaReZ (BoW; le terme «*warez*» signifie logiciel piraté, et l'acronyme BoW vise à tourner en dérision, pour le seul plaisir de la chose, les groupes de *warez* actifs sur *bulletin board system* [BBS], sorte de forum). Selon un ancien membre du BoW avec qui j'ai chatté, l'«aile paramilitaire» du groupe, Hagis (acronyme de *Hackers Against Geeks in Snowsuits*, hackers opposés aux geeks en combinaison de

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

ski), menait des campagnes de hacking cruelles dont les victimes pouvaient être des entreprises, des *white hats** (chapeaux blancs), des gourous de la sécurité informatique ou quiconque se trouvait sur son chemin. À la fin des années 1990, par exemple, une querelle de plusieurs années qui opposait les membres de Hagis à un *white hat* nommé Jay Dyson a violemment dégénéré. Les Hagis se sont d'abord attaqués à son fournisseur d'accès internet en effaçant l'intégralité de ses fichiers, ce qui a contraint Dyson à rester hors ligne pendant deux semaines. Puis, ils ont supprimé des fichiers sur le site professionnel de Dyson. Enfin, pour faire bonne mesure, ils se sont mis à harceler sa femme en lui envoyant des menaces par l'entremise de son propre compte courriel, qu'ils avaient piraté: «Toute la famille Dyson va payer pour les erreurs de Big Jay[17].»

Quand l'ex-membre du BoW avec qui je chattais m'a raconté cette affaire et d'autres attaques auxquelles il avait pris part, je lui ai répondu:

> <biella> ça alors, impitoyable
> <hacker> ouais, nous étions vraiment vaches, tellement que j'ai fini par quitter le milieu
> <biella> pourquoi? enfin, qu'est-ce qui vous motivait? vous le faisiez simplement parce que vous le pouviez?
> <hacker> j'en ai aucune idée
> <hacker> y avait des guerres féroces entre les hackers et personne était au courant
> <hacker> des serveurs irc disparaissaient, des fai étaient rayés de la carte pendant plusieurs jours ou semaines
> <hacker> mais ça sortait pas du milieu
> <hacker> c'est à peine si les médias s'en apercevaient
> <hacker> à l'époque, les hackers ne cherchaient pas à attirer l'attention, ceux qui parlaient aux médias se faisaient traiter de putes
> <hacker> on formait une authentique sous-culture, avec ses propres infos, célébrités, jargon, bref sa propre culture

Je n'ai pu m'empêcher d'ajouter:

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<biella> et ses propres guerres

Néanmoins, les membres de Hagis savaient parfois se montrer beaux joueurs. Un jour, ils ont défacé* le site web de Greenpeace en y affichant un message (qui serait aujourd'hui considéré comme typique du *lulz*) dans le but de sensibiliser le public au calvaire d'un *phreaker* et hacker qui venait de se faire arrêter: «Si Kevin Mitnick n'est pas libéré, nous assommerons 600 bébés phoques[18].»

Après avoir ainsi creusé le sujet (c'est-à-dire, il faut bien l'avouer, quasiment pas), je me suis dit que mes interlocuteurs avaient raison: il était temps pour moi de tempérer mes recherches sur u4ea. Si presque rien n'avait été écrit sur ce troll célèbre, ce n'était pas pour rien.

Dans les années 1990, une autre voie a aussi mené le trollage à l'anonymat. Ignorant tout des guerres secrètes entre hackers d'élite, les utilisateurs lambda ont eu leur premier avant-goût – amer – du trollage sur Usenet, ce mégaforum électronique, premier de son espèce. En 1979, en effet, internet était encore un réseau strictement universitaire et militaire, ARPANET, dont l'accès était réservé à quelques privilégiés. Tout naturellement, un petit groupe d'ingénieurs avait créé un nouveau réseau, Usenet, qualifié d'«ARPANET du pauvre». Pensé dans le seul but de faciliter d'obscures discussions techniques, le réseau avait vite pris de l'expansion (à la surprise de tous les observateurs) pour accueillir des centaines de listes où avaient lieu de vifs débats, parfois houleux. Aux sujets techniques s'étaient peu à peu ajoutés des thèmes comme la sexualité, l'humour, la cuisine et (bien sûr) la dénonciation de la Scientologie.

C'est sur Usenet (et d'autres listes de diffusion) que le terme «troll» est passé dans l'usage courant. Il désignait des gens qui ne participaient pas de façon constructive aux discussions, qui ergotaient pour ergoter ou qui se comportaient en véritables goujats (consciemment ou non). Des utilisateurs incitaient souvent leurs interlocuteurs à «ne pas nourrir le troll», un avertissement courant encore de nos jours sur les listes, les forums et les commentaires des sites.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Mais Usenet a aussi favorisé l'avènement et l'essor d'une espèce spectaculaire de trolls qui sabotent, eux, *volontairement* les conversations, suscitant l'exaspération des utilisateurs et, plus particulièrement, des administrateurs de listes. On ne pourrait trouver meilleur exemple de ce phénomène que Nétotchka Nezvanova, dont le nom, inspiré du personnage éponyme d'un roman (inachevé) de Dostoïevski, signifie «moins-que-rien sans nom». Tout comme Anonymous aujourd'hui, ce nom aurait été utilisé par bon nombre de personnes et de groupes différents, ce qui en fait un exemple pertinent de ce que le spécialiste des médias Marco Deseriis qualifie de «nom à usages multiples», où «un même pseudonyme» est adopté par des «collectifs organisés, des groupes d'affinités et des auteurs individuels»[19].

Publié en ligne, le manifeste artistique de Nétotchka Nezvanova rend bien compte du style intense et délirant du personnage:

> InterCorps: Manifeste artistique
>
> Internet: lieu où l'on peut avoir accès au projet + au matériel adéquat
>
> Nos corps sont les frontières de notre compréhension. Les univers sont le corps. Internet est la peau. Voici mon InterCorps. Je suis programme [*Soft Wear*].
>
> Quand je suis seule, je veux que vous entriez en moi, je veux vous porter [*wear you*].
>
> Dissous et intégrés, nous sommes éclatés en une topologie nomade et instable de rubans de céramique et de canaux microfluidiques,
> de la myriade de lueurs phosphorescentes de transpositions inattaquables
> de signes visibles de rencontres invisibles et mystérieuses dans des rêves divisibles.

On peut apprécier, comme je l'ai fait, la sensibilité imaginative et deleuzienne d'un tel texte – sauf à faire partie d'une des listes de diffusion auxquelles Nétotchka Nezvanova s'est attaquée. Devant les perturbations

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

aussi habiles que fréquentes auxquelles elle se livrait sur des forums très divers, des administrateurs se sont créé une liste spécifique dans le seul but de gérer cette vague de destruction. À l'Université McGill, où j'enseigne aujourd'hui, Nezvanova a participé pendant un temps à une liste de diffusion sur Max, un langage de programmation visuel destiné à la musique et au multimédia. Elle en a été chassée en 2001 après qu'elle en eut menacé certains membres. Voici une partie des motifs invoqués pour justifier son expulsion:

> Deuxièmement, après qu'«elle» a été bannie de la liste de McGill, «elle» a lancé une véritable campagne de terreur: envoi de pourriels à quiconque publiait quelque chose sur la liste Max, attaques par saturation, envoi de messages menaçants et diffamants à des membres de la communauté universitaire choisis au hasard... Ni moi ni mes collègues ne méritons de subir un tel harcèlement. Or il se trouve qu'une bonne partie de ces actes sont criminels. Si «elle» devait récidiver, ses victimes pourraient décider de porter plainte, et je leur recommanderais vivement de le faire.

Un membre de la liste a vivement réagi: «Bon, revoilà la censure[20]!»

Dans les années 1990, Usenet et les autres listes de diffusion, alors en plein essor, encourageaient une liberté d'expression sans restrictions, ce qui leur valait maints éloges. Mais les trolls comme Nétotchka Nezvanova ont forcé un débat de fond, qui a encore cours aujourd'hui, sur les limites de cette liberté: les modérateurs de listes et de forums devraient-ils endiguer les propos offensants au nom de la civilité, considérée par certains comme essentielle à la santé d'une communauté? Ou devraient-ils plutôt se garder de toute forme de censure, quelle que soit la teneur du discours, afin qu'internet reste un espace où la liberté d'expression règne sans condition?

Toute généalogie du trollage doit porter une attention particulière à 4chan, un *imageboard** inspiré du site japonais Futaba, aussi appelé 2chan («chan» est l'abréviation de *channel*, canal). C'est là, sans doute plus que n'importe où ailleurs, qu'est apparu ce genre de trollage aujourd'hui bien connu. 4chan se distingue par sa culture d'une extrême permissivité (tout

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

débat sur la liberté d'expression y est dépourvu de pertinence), favorisée par l'anonymat de ses utilisateurs. Tout naturellement, c'est sur ce forum que le projet collectif et l'identité d'Anonymous ont vu le jour. Contrairement aux gens qui fréquentent Usenet, aucun des participants à 4chan n'est un tant soit peu indisposé par les propos inconvenants qui s'y répandent à toute heure du jour. À maints égards, le site a été explicitement conçu comme une zone où l'on peut dire n'importe quoi: plus c'est grossier, mieux c'est.

Depuis son lancement en 2003, 4chan est devenu un *imageboard* emblématique. Immensément populaire, les contenus choquants n'y manquent pas. Constitué d'une soixantaine de forums dont les thèmes vont des *anime* à la santé, il est la source d'objets culturels parmi les plus chéris d'internet (tels les *lolcats*) autant que de certaines de ses obscénités les plus infectes. Le forum Random (aléatoire), aussi appelé /b/, regorge de pornographie, d'injures racistes et d'une forme particulière d'humour irrévérencieux. Les trolls y ont longtemps prospéré. Un «/b/tard» (gentilé des habitants du forum) a expliqué à mes étudiants que «tout le monde devrait savoir que /b/ est un foutoir pratiquement sans filtre où on peut voir tout ce qui est imaginable et plein de trucs qu'on n'oserait même pas imaginer». On peut y trouver par exemple la photo d'une femme nue avec pour légende «Évaluez ma femme». Ou une insupportable image d'un corps affreusement mutilé. Mais le tout peut être suivi d'une perle d'humour bon enfant:

Fichier: 1291872411.jpg (10 KB, 292x219, bicarbonate-de-sodium.jpg)

☐ **Anonyme** 09/12/10(jeu)00:26:51 N° 293326XX
Je viens de bouffer une demi-cuillère de bicarbonate de soude je fais quoi?

☐ **Anonyme** 09/12/10(jeu)00:28:24 N° 293326XXX
bump

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

☐ **Anonyme** 09/12/10(jeu)00:29:12 N° 283326XXX

>>293326451

c'est pas beaucoup. je te suggère de boire de l'eau. puis de roter.

☐ **Anonyme** 09/12/10(jeu)00:33:06 N° 293327XXX

FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF MANGE PLUS, AVALE DU COLORANT ALIMENTAIRE ROUGE AVEC DU VINAIGRE, ATTENDS LA RÉACTION PUIS COURS DANS LA PIÈCE PLEINE DE MONDE LA PLUS PROCHE EN CRIANT «JE SUIS LE DIEU DES VOLCANS TOAN GLADIUS! BLBLBLBLBLBLBLBLBL!»

Le plus souvent, toutefois, le contenu se veut délibérément outrageant pour les étrangers au forum, sorte de muraille discursive destinée à tenir les non-initiés (appelés *n00bs* ou *newfags*) le plus loin possible. (À peu près tout le monde, des vieux routiers aux néophytes, est qualifié de *fag**, qui signifie littéralement «pédé»; le suffixe apparaît à maintes reprises dans ce livre.) Pour les initiés, il s'agit là du cours normal des choses, une des caractéristiques – et un des attraits – du forum.

Sur 4chan, les participants sont fortement encouragés à ne pas révéler leur identité, si bien que la plupart d'entre eux publient par défaut sous le pseudo Anonyme, comme dans l'exemple ci-dessus. Dans les faits, toutefois, 4chan enregistre les adresses IP de ses visiteurs et ne fait rien pour protéger leur anonymat. Le fondateur, propriétaire et administrateur du site, Chris Poole, peut accéder à sa guise à l'adresse IP d'un utilisateur, à moins que celui-ci ne l'ait masquée avant de se connecter au site. Il a même transmis des adresses aux autorités dans le cadre d'enquêtes officielles (cette politique est connue de la plupart des utilisateurs). Néanmoins, en pratique (du moins entre utilisateurs), le forum est anonyme. Sauf en de rares exceptions, comme dans les cas particuliers où un sujet de discussion doit être identifié par une photo datée, les participants interagissent sans pseudo ni nom d'usager. Les publications sont chassées de la page d'accueil très rapidement et sont supprimées du serveur lorsqu'elles atteignent la page 14; elles ne persistent que si l'intérêt des utilisateurs se maintient. Cette politique «atténue la responsabilité personnelle et encourage l'expérimentation», observe le spécialiste des médias Lee Knuttila[21].

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

L’expérimentation prend la forme de mèmes*, d’impitoyables campagnes de trollage orchestrées par Anonymous (qui se sont faites plus rares cependant ces dernières années) et de railleries incessantes entre utilisateurs (comme d’encourager un participant aux idées suicidaires à «passer à l’acte» en vue de devenir «un héros»). Il faut cependant souligner une profusion de conseils empreints de compassion et d’empathie, destinés en particulier aux personnes ayant besoin d’aide dans leurs relations ou à celles qui sont tombées sur une vidéo de mignon petit chat se faisant torturer. Mais les médias mentionnent rarement cet aspect.

Toutes ces publications sont éphémères, ce dont les utilisateurs sont parfaitement conscients. Contrairement à beaucoup de listes de diffusions et de forums, 4chan n’archive pas les échanges. Si, après un certain temps, un fil n’est pas ramené à l’avant-plan par une réponse, il s’éteint et disparaît. Sur un forum actif comme /b/, le cycle de vie ne totalise que quelques minutes.

Dans ce contexte, on peut difficilement se forger une réputation ou devenir célèbre. Néanmoins, sur cette toile de fond nourrie d’expérimentations aussi cacophoniques que fugaces, une mémoire et une identité collectives solides se sont constituées autour de campagnes de trollage légendaires, de blagues entre initiés ou d’artefacts comme les mèmes visuels. Sur le plan esthétique, plus un contenu est outrancier, meilleur il est, car il éveille l’intérêt des participants et suscite des réponses aux fils de discussion (ce qui les maintient actifs). S’il est particulièrement novateur, un contenu outrancier peut même sortir des limites du forum pour atteindre les terres lointaines de forums web, de Reddit ou de Bodybuilding.com, puis aboutir dans la culture de masse. N’oublions pas que les *lolcats* ont vu le jour sur 4chan! Les trolls, en particulier, consacrent leurs énergies à la quête collective de victoires héroïques, qui, à leurs yeux, représentent simplement une forme de contenu parmi d’autres. (Précisons que, si 4chan héberge de nombreux trolls, une bonne partie de ses utilisateurs évitent cette activité, voire ne font rien du tout, se limitant à observer les autres.)

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Il est presque impossible de cerner avec précision le moment où le trollage a commencé sur 4chan. On sait toutefois que, en 2006, le nom d'Anonymous était déjà utilisé lors de raids menés par des trolls. De telles invasions se sont poursuivies pendant plusieurs années, même après le virage militant du collectif. En 2010, par exemple, Anonymous a entrepris de «ruiner» la vie d'une pré-adolescente, Jessi Slaughter de son pseudo, après que les vidéos maison de ses monologues, qui lui avaient valu une certaine notoriété sur des sites de commérage pour ados comme StickyDrama, furent publiés sur 4chan. Exaspérés par les fanfaronnades éhontées de Slaughter (dans une de ses vidéos, elle annonce qu'elle va «vous foutre un Glock dans la bouche et réduire votre cervelle en bouillie»), les Anons ont publié son numéro de téléphone, son adresse et son nom d'utilisatrice Twitter, l'ont inondée de courriels haineux et d'appels téléphoniques menaçants, et ont fait circuler des photos d'elle retouchées et des parodies de ses vidéos. Quand son père y est allé de son propre coup de gueule, où il prétendait avoir «retracé» ses persécuteurs et les avoir dénoncés à la «cyberpolice», il a été tourné en ridicule à son tour. Qualifiée de «vache *lulz*... pute» par les /b/tards, Slaughter est maintenant immortalisée dans l'*Urban Dictionary* en tant qu'«exemple même de la pute/poseuse/laissée-pour-compte/punkette de 11 ans qui rêve de célébrité».

D'un côté, ces campagnes de trollage excentriques, ajoutés aux propos dégradants (tels que «vache *lulz*» ou le «pour cause de faillite et de sida» des raids contre Habbo Hotel), offrent aux utilisateurs de 4chan un puissant répulsif qui éloigne les internautes naïfs de *leur* terrain de jeux. De l'autre, comparé à la plupart des viviers pour trolls (telle la GNAA de weev), 4chan est La Mecque du trollage «populaire». Par populaire, j'entends simplement que 4chan est accessible à quiconque est disposé à découvrir cet univers, à prendre le temps de s'en approprier l'argot et (évidemment) à en supporter le côté sordide. Les mœurs et les pratiques des utilisateurs du forum ne sont élitistes qu'en apparence. Un de mes anciens étudiants m'en a donné l'aperçu qui suit. Remarquablement intelligent, il était aussi un troll – ou plus précisément un *goon* (voyou), car c'est ainsi que se présentaient les utilisateurs de Something Awful, un site alors très apprécié des trolls:

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> Something Awful (SA) est comme le *country club* exclusif d'internet, avec ses frais d'adhésion de dix dollars, sa liste de règles particulières, ses modérateurs chargés d'interdire et d'homologuer et ses «bonnes publications» garanties par une communauté qui n'a pas peur du ridicule. 4chan, en revanche, est un chaos organique où l'on accorde moins d'importance aux règles qu'à la mégalutte à mort qu'on y mène pour la meilleure blague. N'importe qui peut y participer, et personne ne peut y devenir célèbre comme sur SA, car tout le monde s'y exprime dans l'anonymat.

À tout ce qui se déroule sur 4chan (qu'il s'agisse d'une blague, d'une longue conversation ou d'une campagne de trollage de trois jours), l'anonymat est essentiel. Ce dernier peut être considéré à la fois comme sa règle de base et son trait culturel dominant – dont a hérité Anonymous jusque dans son incarnation en hordes de porteurs de masques de Guy Fawkes. 4chan est le lieu d'une interaction entre la *fonction* de l'anonymat (qui rend possible une compétition pure, non altérée par la réputation ou le statut social) et ses *effets* (les mèmes, les hacks et les trolls, dont l'empreinte sur le monde est bien réelle). Contrairement aux sales coups égocentriques d'un weev, les actions collectives de la «machine de haine d'internet» d'Anonymous déchargent ceux qui y prennent part de toute responsabilité au sens individuel du terme, mais pas au sens collectif. Anonymous est ouvert à quiconque est prêt à se fondre dans un groupe dont la renommée découle d'opérations comme les raids contre Habbo Hotel. N'induisant aucune reconnaissance individuelle, chaque action est attribuée à un pseudonyme, à une réincarnation de Nétotchka Nezvanova. Les utilisateurs de 4chan se moquent d'ailleurs des gens qui rêvent d'attention et de célébrité, qu'ils appellent les *namefags*.

Comme groupe de trolls, Anonymous a acquis une notoriété considérable, tout comme weev. Le collectif est en quelque sorte devenu célèbre. Toutefois, bien que les campagnes de trollage d'Anonymous et des autres utilisateurs de 4chan, d'une part, et de weev, d'autre part, fassent appel à des stratégies similaires, elles sont aussi antinomiques. Quel que

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

soit le degré de célébrité d'Anonymous, l'identité individuelle de ses membres demeure subordonnée à l'intérêt du collectif pour les victoires héroïques et, surtout, pour le *lulz*[22].

Une telle subsomption de l'identité individuelle sous l'identité collective est inusitée dans la culture occidentale. Il est essentiel d'en saisir la logique pour comprendre comment Anonymous est devenu un groupe militant. Il est fort probable que la nature répugnante du trollage de ses débuts ait motivé ses membres à se cacher derrière le collectif par souci de sécurité. Les Anons ressentaient sans doute le désir d'y participer – et d'y gagner en *lulz* – sans risquer d'être reconnus et stigmatisés. Pour comprendre leurs motivations et l'importance que revêt pour un individu le fait d'être disposé à fondre son identité dans celle d'un groupe, penchons-nous brièvement sur la culture de la célébrité individuelle.

Se moquer de la célébrité individuelle par la célébrité collective

La quête de la célébrité est omniprésente dans l'Amérique d'aujourd'hui, des médias de masse qui confient leurs bulletins de nouvelles à des stars d'Hollywood aux micromédias en ligne, propices à un déferlement de narcissisme et d'autoglorification, en passant des universités, où des professeurs vedettes réclament des salaires considérables, aux stades, où les sportifs touchent des revenus obscènes. Cette soif de renommée renforce ce que l'anthropologue David Graeber, s'appuyant sur les travaux précurseurs de C.B. Macpherson, qualifie d'«individualisme possessif», défini comme «ces façons profondément ancrées de penser et de ressentir» par lesquelles nous considérons «tout ce qui nous entoure comme une propriété commerciale réelle ou potentielle»[23].

Comment 4chan, un des recoins les plus sordides d'internet, a-t-il pu faire éclore, sans que ses membres en aient eu la moindre intention, une incarnation à ce point robuste d'une éthique collectiviste dressée contre la célébrité? Si une telle éthique a pu prospérer spontanément sur ce forum,

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

c’est parce qu’elle s’est manifestée à l’état pur. À mes étudiants, un ancien troll d’Anonymous devenu activiste a expliqué le rôle crucial joué par 4chan dans l’émergence de ce qu’il a qualifié d’«idéal fondamental d’Anonymous»: «Les messages publiés sur 4chan sont dépourvus de nom ou de quelque autre marque permettant d’en identifier l’auteur. On peut donc juger une publication uniquement sur son contenu. *Cette absence de personnalité et, par le fait même, de tout ce qui vient avec, comme l’autorité, la représentation et le statut social, est l’idéal premier d’Anonymous.*» (C’est moi qui souligne.)

Cet Anon, qui s’adressait de façon anonyme, par Skype, à mes dix étudiants ravis, a brillamment qualifié cet idéal d’auto-effacement de l’individu. Quand Anonymous a quitté 4chan pour se consacrer à ses projets militants en 2008, a-t-il expliqué, l’idéal s’est étiolé, parfois de façon spectaculaire: aussitôt que ses membres ont commencé à interagir en s’identifiant par des pseudonymes ou en personne, leur désir de statut social s’est manifesté; ils se sont mis à manœuvrer et à se bousculer pour le pouvoir.

Néanmoins, le tabou de la recherche de célébrité, profondément enraciné sur 4chan, était encore considéré d’un très bon œil en raison de ce qu’il avait permis d’accomplir. À quelques exceptions près, il a donc largement empêché les luttes intestines de donner lieu à l’expression publique d’ambitions personnelles. (Plus loin, nous nous pencherons sur son échec retentissant dans de petites équipes de hackers comme AntiSec et LulzSec, qui ont acquis célébrité et reconnaissance à la manière de vedettes rock et ont suscité, sans surprise, la colère de certains Anons tout en étant admirées pour leurs facéties politiques empreintes de *lulz*.)

Lorsque les membres d’Anonymous ont tourné le dos à 4chan pour se vouer à l’activisme, leur refus de la célébrité est devenu «plus nuancé [...], s’incarnant dans un désir de ne pas avoir de chef et une aspiration à la démocratie directe», comme l’a expliqué mon Anon. Les tentatives de mettre ces principes en pratique ont suscité leur lot de faux pas, notamment dans l’émergence de petites équipes où se concentrait le pouvoir.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Malgré cette fragmentation en équipes et ces rivalités, les grands idéaux sont restés vivants. L'adhésion au collectif reposait sur le principe selon lequel «n'importe qui [pouvait] revendiquer le nom d'Anonymous, en toute légitimité», a poursuivi mon conférencier. C'est précisément cette liberté d'agir en brandissant ce nom qui a permis à Anonymous de devenir l'hydre qu'il est aujourd'hui.

Cependant, si l'on gratte un peu derrière l'idéal (l'idée voulant qu'Anonymous appartienne à tout le monde et que cette identité soit en quelque sorte un bien commun), on découvre une réalité beaucoup plus complexe. C'est sur cet avis nuancé que l'Anon a conclu sa brève présentation. Mes étudiants étaient à la fois fascinés et stupéfaits de constater qu'un Anon puisse se montrer si brillant et si éloquent. Je leur ai expliqué que les membres du collectif pouvaient être considérés comme ce que l'anthropologue Christopher Kelty désignait à la blague sous le nom de «superalternes», par opposition à subalternes: des geeks fort instruits qui, en plus de pouvoir très bien défendre leurs positions, répliquent avec vivacité et esprit critique à quiconque prétend parler en leur nom[24]. Le conférencier d'Anonymous a fini par ajouter:

> La plupart d'entre nous sommes motivés par l'humour. C'est pourquoi il ne faut pas s'étonner de nos disputes fréquentes avec des groupes qui, tout en se réclamant d'Anonymous, n'ont plus nos bonnes grâces, comme [...] les nouveaux Anons strictement militants d'Occupy Wall Street, les adeptes des théories du complot ou d'autres entités beaucoup trop sérieuses qui se parent de ce nom. C'est vrai. Nous ne pouvons pas les empêcher d'utiliser notre nom. Il importe cependant de retenir que notre idéal ne stipule nullement qu'Anonymous doive être solidaire des autres Anonymous ou même les apprécier. En fait, l'animosité et les guerres ouvertes entre groupes se réclamant d'Anonymous s'inscrivent dans la droite ligne des actions menées sur internet par les premiers représentants de la culture Anon.

C'est ici qu'on peut saisir toute la complexité d'Anonymous. Le collectif est animé par une idée singulière, que ses membres cherchent à concrétiser

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

en un front uni. Pour les médias, il est tentant de s'en tenir à cette image de marque en réduisant Anonymous à ses valeurs et à son emballage. Toutefois, même si le mouvement utilise un seul nom, il est impossible d'en esquisser la réalité dans toutes ses nuances, car il est constitué de trop de réseaux et de sous-groupes différents, auxquels il arrive parfois d'être en désaccord entre eux. Fondamentalement, pour ce collectif de collectifs, l'accumulation d'un trop grand pouvoir ou d'un trop grand prestige (en particulier en un endroit précis de l'espace virtuel) est non seulement tabou, mais aussi problématique sur le plan fonctionnel.

4chan aura été la matrice d'une éthique réfractaire à la célébrité, à un système de valeurs hostile à l'autoglorification et aux grands médias (qui font partie des cancers en train de tuer /b/, aiment à dire les Anons). Cette éthique a trouvé son prolongement dans le virage militant d'Anonymous. C'est dans ces formes nouvelles de sociabilité (qui ébranlent la division idéologique entre l'individuel et le collectif) qu'on peut reconnaître la transformation du trollage en une arme, dont l'utilisation obéit à des principes, contre les grandes banques et les firmes de sécurité louches. L'esprit collectif marque des points: au mouvement antimondialisation apparu au tournant du siècle se sont ajoutés Anonymous et une multitude de groupements sans têtes dirigeantes comme Occupy. Les manifestations de ce phénomène échappent souvent aux grands médias: ces derniers sont incapables (ou n'ont pas l'intention) de produire un reportage qui ne présente pas comme allant de soi l'accession d'une personne au statut de célébrité ou de chef, avec son héroïsme individuel ou ses accrocs à la morale. Cette propension n'est évidemment pas exclusive aux journalistes. Pour l'essentiel, la philosophie et, de façon plus générale, la culture occidentales postulent que l'individu est l'objet essentiel de la recherche épistémique. Une pensée philosophique millénaire intégrée au sens commun ne se laisse pas ébranler facilement.

C'est pour cette raison qu'Anonymous, tant dans sa variante trolle qu'activiste, déploie son être-*trickster* en usant de méthodes dignes du jiu-jitsu. Ses tactiques sont sans commune mesure avec la logique des grands médias et la sensibilité individualiste dominante. Le collectif rend les

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

journalistes un peu dingues (ce dont j'ai été le témoin direct quand j'ai joué l'intermédiaire entre Anonymous et les médias, faisant un peu une *trickster* de moi-même). Je les ai souvent aidés à franchir le gouffre à petits pas, alors qu'ils cherchaient un chef, ou à tout le moins un personnage qui leur aurait permis de satisfaire aux exigences implicites de leur métier.

C'est sans doute en raison de cette résistance aux conventions journalistiques (au désir de trouver un dirigeant et de le rendre célèbre, voire d'en créer un de toutes pièces s'il le faut) que les journalistes détestent couvrir Anonymous. Leur chasse au porte-parole, au chef, au représentant est longtemps restée vaine, du moins jusqu'à ce que l'État se jette dans la mêlée en se mettant à arrêter des hackers. Dans l'ensemble, les médias n'ont guère déniché de personnages à propos desquels il leur aurait été facile de pondre des reportages.

Ce qui a débuté comme un réseau de trolls est devenu une force essentiellement consacrée au bien commun. L'émergence d'Anonymous dans un des milieux les plus sordides d'internet est un conte empreint de merveilleux, d'espoir et de joyeuses illusions. Est-il vraiment possible que ces idéaux collectifs, tels qu'ils ont pris forme dans l'enfer du trollage, aient su transcender ces origines? Le cloaque de 4chan s'est-il vraiment mué en un des groupes militants les plus politiquement actifs, moralement fascinants et subversivement nécessaires aujourd'hui en activité? Réponse plutôt surprenante: oui. Voyons comment.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Chapitre 2

Opération Chanology: «J'suis venu pour le *lulz*; j'suis resté pour la cause»

DIVERS ALÉAS ONT CONCOURU À L'ÉVEIL des *tricksters*-trolls qui rampaient dans les bas-fonds glauques de 4chan. Mais si un événement s'est avéré plus déterminant que les autres, nous l'avons mentionné, c'est bien la diffusion sur internet d'une vidéo de l'Église de scientologie qui mettait en vedette Tom Cruise, porte-flambeau le plus célèbre de la secte. L'«effet Streisand à plein régime», lancerait plus tard un Anon d'un ton malicieux, faisant référence à ce phénomène, courant sur internet, par lequel une tentative de censurer un document produit l'effet inverse: curieux de connaître les motifs de la censure, les gens se bousculent pour avoir accès au document en question, qui finit par se répandre beaucoup plus largement que si on ne s'en était pas soucié. Ce phénomène doit son nom à un épisode de 2003 où Barbra Streisand avait tenté, par l'entremise d'une poursuite judiciaire de plusieurs millions de dollars, d'interdire la publication de photos aériennes montrant sa résidence de Malibu. Le photographe incriminé avait simplement voulu documenter l'érosion littorale. Avant la poursuite, l'image n'avait été vue que 6 fois en ligne; une fois celle-ci rendue publique, le site a reçu plus de 420 000 visites. La vidéo scientologique de Tom Cruise allait connaître un sort semblable: sa circulation deviendrait incontrôlable.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Dans ladite vidéo, Cruise offre un parfait exemple de la vision du monde narcissique de l'Église de scientologie: «Quand on est scientologue [...] et qu'on est témoin d'un accident, on ne fait pas comme tout le monde», y explique-t-il avec un sourire de satisfaction. «En s'approchant, on sait qu'on doit faire quelque chose, car on est conscient d'être la seule personne en mesure d'apporter une aide véritable.» Les geeks (et presque tous les autres internautes) ont perçu ce bout de film comme une tentative pitoyable (pour ne pas dire à se tordre de rire) de donner de la crédibilité à une pseudoscience en misant sur une célébrité. Alors, tandis que Cruise gloussait, la communauté des internautes s'est mise à glousser avec lui – mais pour de tout autres raisons.

La vidéo n'a pas atterri sur internet par les soins d'Anonymous, mais par une fuite anonyme survenue avec grand à-propos. NBC avait envisagé de la diffuser à l'occasion de la parution d'une biographie non autorisée de Tom Cruise, mais, à la dernière minute, la chaîne s'est dégonflée. Les pourfendeurs de la Scientologie se sont alors empressés de lui frayer un chemin vers le web. De concert avec Patricia Greenway, une ancienne membre de la secte devenue une farouche opposante, Patty Moher a fait parvenir une copie de la vidéo par FedEx au reporter Mark Bunker, qui l'a mise en ligne sur son site. Bunker a envoyé le lien au journaliste d'enquête Mark Ebner, qui l'a fait suivre à son tour à d'autres médias. Le 13 janvier 2008, *Gawker*, *Radar* et d'autres sites ont repris l'information en y incluant le lien de Bunker, qui croyait avoir verrouillé la vidéo avec un mot de passe, mais avait omis de le faire. «En me réveillant quelques heures plus tard, j'ai constaté que la séquence où se trouvait le monologue de Cruise n'avait pas été réglée sur "confidentiel"», raconterait-il par la suite. «Elle avait été visionnée 20 000 fois pendant mon sommeil, et des gens qui avaient lu les articles de *Gawker*, de *Radar* et d'autres médias l'avaient partagée à l'infini[1].» YouTube a fini par retirer les vidéos de la chaîne TomCruiseBook – et par éliminer la chaîne elle-même –, sans doute à la demande de l'Église de scientologie, qui aurait fait valoir son droit d'auteur.

Le 15 janvier, *Gawker* republiait la vidéo en l'accompagnant d'une légende brève et incisive, au goût de ses millions de visiteurs: «Disons que,

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

si Tom Cruise sautant à pieds joints sur le canapé d'Oprah atteint 8 sur l'échelle de l'épouvante, cette vidéo vaut un 10.» Le Religious Technology Center (division de la secte chargée des questions de propriété intellectuelle) a réagi sans attendre en mettant l'éditeur en demeure de retirer la vidéo sous peine de poursuite. *Gawker* concluait son article non sans effronterie: «La vidéo détient un intérêt journalistique. Nous n'entendons pas la retirer[2].» La mèche était éventée; l'Église de scientologie était furieuse (et s'apprêtait à intenter des poursuites judiciaires). L'enfer se déchaînerait quand la «ruche» (comme Anonymous était alors souvent surnommé) déciderait de s'impliquer dans l'affaire.

C'est le 7 janvier à 19 heures 37 minutes et 37 secondes que les portes de l'enfer se sont ouvertes avec le lancement sur /b/ d'un fil de discussion sur le militantisme antiscientologique:

Fichier: 1200443857152.jpg (22 KB, 251x328, intro_scn.jpg)

☐ **Anonyme** 15/01/08(mar)19:37:37 N° 51051816

Le temps est venu pour /b/ de faire quelque chose de gros.

Les gens doivent comprendre qu'ils ne doivent pas faire chier /b/, dire n'importe quoi pendant dix minutes et s'attendre à ce que les gens donnent leur argent à une organisation qui n'a pas un gramme de putain de bon sens.

Je parle de «hacker» ou d'«anéantir» le site internet officiel de la Scientologie.

Il est temps pour nous de consacrer nos ressources à une cause que nous croyons juste. Il est temps de faire quelque chose d'important, /b/.

Parlons-en entre nous, trouvons le meilleur endroit pour planifier ça et faisons ce qui peut et doit être fait.

Le moment est venu, /b/.

Techniquement (et les geeks ont l'habitude de s'attarder aux détails techniques), un appel aux armes avait été publié un peu plus tôt sur 4chan et sur 711chan (à 18 h 11, m'a-t-on dit). Quoi qu'il en soit, c'est ce fil de discussion qui aurait incité le plus grand nombre de trolls à passer à

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

l'action. Malgré la confiance et l'exubérance (hyperboliques) qui donnaient le ton à la conversation, certains participants se montraient sceptiques à l'idée de s'en prendre à une organisation si puissante – sans parler de l'anéantir –, ce qui se comprend. Ils craignaient que le projet d'attaquer l'Église de scientologie soit «mission impossible»:

> **Anonyme** 15/01/08(mar)19:46:35 N° 51052578
>
> mission impossible
>
> un forum de discussion aléatoire ne peut pas anéantir une pseudoreligion soutenue par des riches et une armée d'avocats
>
> même si chaque personne qui a déjà fréquenté /b/ UNE SEULE FOIS prenait part à une invasion massive, ça resterait sans effet
>
> en plus, si quelqu'un se faisait choper, il aurait 500 avocats au cul avant d'avoir eu le temps de dire «procès»
>
> les scientologues sont réputés pour leur acharnement contre leurs opposants
>
> **Ad** 01/04/07(ven)01:02:07 N° 12345678
>
> **Anonyme** 15/01/08(mar)19:50:22 N° 51052862
>
> »51052482
>
> »51052578
>
> Alors ne participe pas si tu penses que c'est pas possible

Le lendemain, dans un message visionnaire publié sur /b/, un participant lance ce qui deviendrait le cri de ralliement de toutes les opérations anti-Scientologie liées à Anonymous, «CHANOLOGY», et a donné un aperçu des événements à venir:

> Fichier: 1200523664764.jpg (22 KB, 251x328, 120046751294.jpg)
>
> **Anonyme** 16/01/08(mer)17:47:44 N° 51134054
>
> Le 15/1/08, la guerre a commencé.
>
> Le site de la Scientologie subit actuellement des bombardements intenses, il est très long à charger.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Mais ce n'est que la pointe de l'iceberg, le premier d'une série d'assauts. Nous sommes en train de remporter une victoire modeste, mais, sans le soutien solidaire des chans, la Scientologie balaiera cette attaque, dont les seules traces se résumeront à un article dans ED.

4chan, répondez à l'appel! Joignez-vous à la légion dans sa lutte contre la Scientologie, contribuez à son anéantissement, à sa ruine tant attendue! Depuis des décennies, cette secte impose sa tyrannie en corrompant l'esprit des faibles. On peut en rire, mais c'est franchement pathétique. Nous devons enrayer ce mal et lui substituer un mal plus grand encore: la CHANOLOGIE. Car si nous sommes victorieux, les chans, unis, pourront entreprendre un nouveau chapitre de leur existence anonyme, tissée d'insanités sans nom; nous aurons fait un pas vers la domination du monde. Si nous pouvons détruire la Scientologie, nous pourrons détruire tout ce que nous voudrons! Le monde ne sera plus que notre jouet.

Faites votre devoir, 4chan. Ne vous contentez pas de prendre part à la guerre: devenez-en les héros! Vous, la masse des chans, vous pouvez constituer les effectifs dont la légion a tant besoin.

EN AVANT, ANONYMOUS! UNIE, LA LÉGION EST INVINCIBLE

tl;dr nous démolissons la Scientologie, joignez-vous à nous ou foutez le camp

Aucun scifag ne sera toléré sur ce fil de discussion.

http://711chan.org/res/6541.html

Avant que quiconque ait eu le temps de dire «*Ave* Xenu» (Xenu étant, selon la Scientologie, l'infâme dictateur extraterrestre de la galaxie), ces trolls (que je suivrais peu après) se sont branchés au réseau Internet Relay Chat (IRC) Partyvan (très fréquenté par les Anons) pour assister à l'«explosion» des festivités. Ou, à tout le moins, comme l'expliquerait l'un d'eux à mes étudiants:

> Réunis dans d'immenses forums, nous nous sommes coordonnés pour nous livrer à diverses formes de «salopage ultracoordonné sur internet». Pendant de brèves périodes étalées du 15 au 23 janvier, nous avons hacké les sites web de la Scientologie et y avons mené des attaques par saturation en vue de les rayer de la carte. Nous avons bombardé les lignes spéciales de la Dianétique de canulars téléphoniques. Nous avons faxé des feuilles de papier complètement

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> noires à tous les numéros qui nous tombaient sous la main, et nous avons étalé les «secrets» de leur religion partout sur internet. De mon côté, j'ai numérisé mon cul et leur ai faxé le résultat. Parce qu'ils font chier.

Alors que cette bataille héroïque prenait forme sous mes yeux en temps réel, il m'était facile de comprendre pourquoi les geeks et les hackers d'Anonymous s'en prenaient à la Scientologie: celle-ci, en fait, constitue leur double maléfique. Car je ne m'étais pas branchée à ce canal IRC par hasard, j'étais déjà bien au fait des tensions culturelles entre geeks et cybercitoyens, d'une part, et scientologues, d'autre part. Un an auparavant, je vivais à Edmonton, ville canadienne parmi les plus froides où on a l'impression d'être aux confins les plus lointains de l'Amérique du Nord. J'y colligeais des documents appartenant à un fonds d'archives de classe mondiale sur la Scientologie, constitué par Stephen Kent, professeur de sociologie à l'université de l'Alberta. Mes recherches portaient sur un combat épique entre geeks et Église de scientologie. Ce conflit, qui finirait par durer au total une vingtaine d'années, avait éclaté au début des années 1990 quand la secte s'en était prise à ses détracteurs, en particulier à ceux qui divulguaient des textes sacrés qu'elle voulait garder secrets. Baptisée avec humour «Internet contre Scientologie» (bien qu'elle fît rage dans le monde réel autant qu'en ligne), la lutte campait les cybercitoyens (qui se vouaient entièrement à la défense de la liberté d'expression) contre l'Église de scientologie (qui se vouait entièrement à l'écrasement de ladite liberté par tous les moyens, légaux ou non), qui cherchait à étouffer la critique et à empêcher la circulation de ses documents sur internet. Mes recherches m'avaient menée à la conviction qu'effectivement, les hackers et les scientologues campent sur des positions diamétralement opposées. Comme une photo et son négatif, chacun des deux camps est le reflet inversé de son antagoniste, son repoussoir idéal.

Prenons le dogme fondamental que proclame une publication du Religious Technology Center, rattaché à la secte: «Comment faire en sorte que la Scientologie continue à fonctionner». On y trouve une prose digne

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

d’un robot de première génération qui se serait retrouvé bloqué dans un coin sans pouvoir se retourner, émettant chaque fois qu’il bute contre le mur:

> Un: Avoir la technologie correcte.
>
> Deux: Connaître la technologie.
>
> Trois: Savoir qu’elle est correcte.
>
> Quatre: Enseigner correctement la technologie correcte.
>
> Cinq: Appliquer la technologie.
>
> Six: Veiller à ce que la technologie soit appliquée correctement.
>
> Sept: S’acharner de toutes ses forces à réduire à néant la technologie incorrecte.
>
> Huit: Anéantir toute application incorrecte.
>
> Neuf: Fermer la porte à toute possibilité de technologie incorrecte.
>
> Dix: Fermer la porte à l’application incorrecte[3].

Au moment où je lisais ces préceptes en 2007, je savais que tout hacker ou geek qui y poserait le regard serait à la fois amusé et scandalisé. La Scientologie baigne dans le secret, les dogmes et dépend de la mise en œuvre d’une (pseudo)science et de technologies (bidon) pour contrôler ses ouailles; le hacking, lui, repose sur la curiosité, le bidouillage et le principe selon lequel c’est l’exploration qui rend la science et la technologie possibles (et vice versa). Le hacker se voue corps et âme à la création et à la programmation de machines les plus perfectionnées qui soient. Artisan par excellence, il est mû par une quête de la perfection, mais abhorre l’idée voulant qu’une technologie puisse être la seule «correcte». En fait, le hacking se situe au carrefour de l’artisanat et de la malice (*craft and craftiness*): création d’une imprimante 3D qui imprime une imprimante 3D; assemblage d’un réseau de machines zombies* qui, pour accroître sa puissance, prend le contrôle de celui d’un autre hacker; conception d’un

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

robot dont la seule fonction consiste à préparer des cocktails dans le but de le présenter à Roboexotica, un festival consacré à la robotique du cocktail qui existe depuis 1999; inventer un langage de programmation appelé Brainfuck, destiné à donner du fil à retordre à quiconque essaie de l'utiliser. Vous voyez le genre.

Une religion qui prétend avoir un accès privilégié à la science et à la technologie au point de se qualifier de «seul groupe sur Terre à disposer d'une technologie efficace qui permette de manipuler les fondements de la vie elle-même et de mettre de l'ordre dans le chaos[4]» ne peut que heurter profondément les hackers. Tout ce que ces derniers attendent de la technologie, c'est qu'elle *fasse quelque chose*, une fonction qu'ils n'attribuent pas à la révélation transcendantale de quelque vérité, mais plutôt à leur propre ingéniosité, à leur capacité à trouver des solutions à des problèmes techniques grâce à l'échange de tuyaux, d'idées et à du codage emprunté à la tonne.

Pour un groupe comme Anonymous, constitué de hackers et de geeks, il était donc tout naturel de s'en prendre à la Scientologie. Mais une question restait en suspens: les Anons trollaient-ils pour le seul plaisir du *lulz* ou menaient-ils une campagne sérieuse? Selon moi, ils n'agissaient pas de façon délibérément militante. Mais un esprit politique soufflait indéniablement sur leurs canaux IRC. La tentative qu'avait faite la Scientologie d'empêcher la diffusion d'une vidéo sur «leur» internet (en particulier d'une vidéo à ce point grotesque) les avait indéniablement – et royalement – foutus en rogne. C'est pourquoi ils se sont mis à inonder les lignes spéciales de la Dianétique, à faire livrer des centaines de pizzas impayées à des églises et à diffuser leurs exploits en temps réel sur 4chan. Au début, toute visée politique semblait fortuite. Après quelques semaines, toutefois, une opération particulière de «salopage ultracoordonné sur internet» a ouvert la voie à un élan militant plus sérieux – quoiqu'irrévérencieux, comme toujours.

Avec la popularité croissante de l'opération Chanology, les canaux IRC #xenu et #target, surchargés, furent vite déclarés inaptes au regard de la visibilité à laquelle les organisateurs aspiraient. Trois d'entre eux partirent

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

donc de leur côté et lancèrent le canal #press. Ce dernier prit vite de l'ampleur pour passer à huit membres, qui créèrent en une nuit ce que l'on considère encore aujourd'hui comme le chef-d'œuvre d'Anonymous. Plus tard, leur équipe finit par intégrer tant de participants que #press en devint chaotique. Certains de ses membres partirent alors pour former marblecake (gâteau marbré), nom inspiré de la pâtisserie que l'un d'eux était en train de manger.

Alors que le clip de Tom Cruise avait une touche à la fois humoristique et hyperbolique, Anonymous a conçu une vidéo ironique, dont le ton était parfaitement représentatif de l'ambiguïté propre aux *tricksters* – à la fois drôle et sérieuse, taquine et menaçante. À la surprise quasi générale, elle a propulsé les interventions du collectif à une tout autre échelle.

La vidéo montre de lourds nuages qui défilent derrière un immeuble de verre ordinaire. Un discours s'amorce. Livré par une voix synthétique, il est néanmoins inspiré d'un certain lyrisme:

> Anonymous en est venu à la conclusion que votre organisation mérite d'être détruite. Pour le bien de vos fidèles, pour le bien de l'humanité – et pour notre plus grand plaisir. Nous allons vous expulser d'internet et procéder au démantèlement de l'Église de scientologie sous sa forme actuelle.
>
> Nous vous considérons comme un ennemi redoutable, et nous n'espérons pas atteindre nos objectifs en peu de temps. Mais vous ne l'emporterez pas éternellement face aux citoyens en colère. Les méthodes qui sont les vôtres, l'hypocrisie ainsi que le mépris dont vous faites preuve à l'égard des lois ont sonné le glas de votre organisation. Vous ne trouverez nulle part où vous cacher, car nous sommes partout. Vous n'avez aucun recours, car, chaque fois qu'un de nos membres tombe au combat, dix autres viennent le remplacer.
>
> Nous savons que d'aucuns risquent de dénoncer nos méthodes en les comparant à celles de l'Église de scientologie, qu'ils annonceront que votre organisation prendra les actions d'Anonymous en exemple des persécutions contre lesquelles vous mettez en garde vos fidèles

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> depuis si longtemps. C'est acceptable aux yeux d'Anonymous. En fait, nous l'encourageons.

Voilà qui était sérieux. Mais une plaisanterie sérieuse. Cette poésie de la révolte était purement rhétorique, mais elle exprimait le *lulz* de façon si puissante et si séduisante qu'elle a contraint les trolls d'Anonymous à assumer leur engagement et à démanteler la Scientologie. À l'instar de tant de *tricksters* avant eux, les Anons se sont pris à leur propre piège. En donnant soudain une portée politique au *lulz*, ils sont devenus eux-mêmes ces *moralfags* et ces *leaderfags* tant honnis. Saisis par un désir de justice purement circonstanciel, ces Anons ont engendré un des mouvements de contestation les plus influents de notre époque.

Les événements se sont enchaînés comme suit. Sans préavis, la vidéo a provoqué un débat entre Anons pour déterminer s'ils devaient prendre la rue pour contester l'Église ou rester fidèles à leur ancrage identitaire dans le *lulz* et les raids informatiques. Le contexte a fait pencher la balance du côté des manifs. «Certains membres pensaient qu'Anonymous ou 4chan ne devaient pas aller manifester, mais l'idée a fait consensus sans trop de difficultés après la diffusion de la vidéo. Le contexte nous semblait tout à fait propice. Nous avions fait la bonne vidéo au bon moment», expliquerait plus tard Gregg Housh, membre fondateur de marblecake ayant participé au montage de l'œuvre.

Cela dit, même si les Anons commençaient à s'intéresser à la contestation sociale, ils ne s'apprêtaient pas pour autant à renoncer au trollage. Ils souhaitaient bien plutôt élargir leur répertoire. Sur IRC, une Anon a bien résumé le spectre de plus en plus large (légalité, illégalité, *lulz*, sérieux) que ces hordes de trolls se sont mis à (ou voulaient) couvrir entre la mi-janvier 2008 et la première manifestation (son pseudo a été modifié):

> <Lulmania> Le meilleur scénario: Anonymous monte des canulars téléphoniques et des attaques par saturation, les gouvernements des États-Unis et de la France réitèrent leurs accusations de fraude, d'évasion fiscale et autres crimes, les pasteurs d'églises locales mettent en garde leurs ouailles contre les dangers de la

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> Scientologie, d'anciens membres et leurs familles témoignent de leur expérience à la télé, des groupes militants organisent des manifestations autorisées, et les médias couvrent tout ce que je viens d'énumérer [...].
> <Lulmania> N'oublions pas qu'il s'agit d'une guerre d'usure. Nous ne pourrons pas ruiner la Scientologie directement. Il s'agit d'attirer l'attention des médias, d'informer le public, de miner la confiance de ses membres, de bousiller sa connexion à internet et au réseau téléphonique, d'empêcher le lavage de cerveau de ses recrues potentielles... et de faire tout cela pour le *lulz.*

Le 24 janvier 2008, Anonymous annonçait que le 10 février serait une journée de protestation. Quelques jours après ce premier appel à l'action, l'opposant à la Scientologie Mark Bunker a profité de ce contexte effervescent pour enjoindre les Anons à recourir exclusivement à des moyens légaux. À l'instar d'Eshu, *trickster* des communications, des chemins et des carrefours, il s'est adressé aux trolls par l'entremise d'une vidéo (nom de Xenu!!) où il faisait leur éloge (le malin) et les invitait à embrasser la cause (nom de Xenu!!). Il espérait ainsi calmer le jeu, réfréner le *lulz* et prier ses nouveaux alliés (avec ô quelle ferveur!) d'éviter toute action directement illégale. Après les événements, dans une longue contribution au forum Why We Protest, Bunker expliquerait ainsi ses motivations: «Après avoir visionné le "Message à la Scientologie" d'Anonymous, j'ai eu peur d'avoir contribué au déclenchement d'attaques qui auraient pu inquiéter des employés de la Scientologie et occasionner des problèmes judiciaires à des Anons. C'est pourquoi j'ai décidé d'adresser mon premier enregistrement à Anonymous[5].»

Même si de nombreux Anons avaient déjà eu ce genre de pensées, ils ne partageaient pas tous l'opinion de ce quinquagénaire grassouillet, qu'ils avaient surnommé le «Sage barbu» en raison de ses airs d'érudit et de sa blanche barbe. (Cela prendrait quelques années avant que des tactiques illégales comme les attaques par saturation soient employées pour des actions politiques, et ce, par de nouveaux réseaux militants.) Néanmoins, il

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

y en a suffisamment qui ont changé leur fusil d'épaule pour s'engouffrer dans la voie du militantisme, les arguments de Bunker ayant aiguillonné Anonymous vers la légalité.

Le gâteau de marbre, qui travaillait d'arrache-pied dans le plus grand secret (bien qu'un petit groupe d'*outsiders* connût son existence), était conscient que pour presque tous les participants potentiels, la contestation était chose parfaitement nouvelle. Si ces nerds*, geeks, hackers et autres trolls du net, dépourvus comme ils l'étaient de la moindre expérience militante, se rendaient en masse à ce rassemblement, le fiasco était presque garanti. Il fallait donc les familiariser avec ce type d'événements, et vite. marblecake a alors décidé de monter un cours intensif sur le déroulement d'une manifestation pacifique. La vidéo, intitulée «Code of Conduct», fut mise en ligne le 1er février 2008. Une voix robotisée y énumère 22 règles. Tous les détails y sont: il y est recommandé de porter des chaussures confortables, de boire beaucoup d'eau, de garder pour soi les blagues de geeks les plus inconvenantes (pour éviter de choquer les badauds), de s'abstenir de toute violence, d'obtenir les permis nécessaires, de scander des slogans accrocheurs et, enfin, de filmer l'événement. Comme marblecake savait que les scientologues tenteraient par tous les moyens (y compris par des photos en haute résolution) d'identifier les manifestants en vue de les harceler par la suite, une règle exhortait ces derniers à se couvrir le visage, tout en précisant (ce qui paraît aujourd'hui ironique) que porter un masque n'était pas nécessaire: «Règle no 17: Couvrez-vous le visage. Il s'agit d'empêcher nos ennemis, les autres manifestants ou les forces de sécurité de vous identifier. Portez un foulard, un chapeau et des lunettes de soleil. Un masque n'est pas nécessaire, d'autant qu'il est interdit dans certaines municipalités pendant les manifestations[6].»

Nécessaire ou pas, le masque serait omniprésent lorsque, quelques jours plus tard, des milliers d'Anons et leurs sympathisants descendraient dans les rues de plusieurs villes du monde. À l'époque, le masque de Guy Fawkes était déjà une icône de la culture pop grâce à la superproduction hollywoodienne *V pour Vendetta*, qui raconte le combat solitaire d'un anarchiste contre un État dystopique orwellien. Ce masque avait aussi

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

circulé sur 4chan, où il était porté par un fameux personnage de mème qui rate tout ce qu'il entreprend, Epic Fail Guy. Relativement répandu, donc, facile à trouver, chargé d'une portée symbolique indéniable (tant dans son contexte originel que dans son utilisation plus récente), le masque de Guy Fawkes allait devenir l'accessoire du jour pour se protéger du regard inquisiteur de la Scientologie. Et il finirait par devenir l'emblème d'Anonymous.

Les événements du 10 février se déroulèrent dans un mélange de contestation politique réfléchie et d'outrance carnavalesque. Pourquoi tant de gens y participèrent-ils? Lors d'une séance de chat à bâtons rompus, un Anon de longue date, membre de marblecake, me donnerait plus tard l'explication suivante (qui me semble juste): «Les nouvelles des premières manifestations de la journée du 10 février 2008, qui avaient eu lieu en Australie, ont eu un véritable effet d'entraînement. [...] Si elles n'avaient pas eu lieu, je crois qu'il n'y aurait pas eu autant de monde dans les rassemblements tenus ailleurs.» Alors que le reste du monde occidental dormait encore, entre 550 et 850 Australiens – vidéos et photos à l'appui – étaient descendus dans les rues, ce qui a eu un effet domino dans les autres pays. À Londres, 600 personnes ont pris part à la manifestation; en Amérique du Nord, des rassemblements ont eu lieu dans de nombreuses petites villes et dans de grands centres urbains comme Los Angeles, où l'événement a attiré 1 000 participants.

Six mois après que Fox News l'eut qualifié de «machine de haine d'internet», Anonymous attirait donc des légions de sympathisants dans les rues (et pas seulement des geeks et des hackers vissés à leur clavier d'ordinateur), lesquels revendiquaient le nom du collectif, son éthique de l'anonymat et son iconographie. Ce soir-là, les journaux télévisés du monde entier montrèrent des hommes et des femmes vêtus de noir, parés de masques de Guy Fawkes et munis de pancartes déclarant «Nous sommes internet».

C'était bien la première fois que les Anons manifestaient en nombre dans les rues, quoique certaines de leurs campagnes de trollage antérieures avaient tout de même eu une dimension quasi militante. Par exemple,

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

lorsqu'Anonymous s'en était pris à l'animateur de radio conservateur Hal Turner en 2007, ce n'était pas seulement pour le *lulz* (ou par esprit de vengeance), mais aussi parce qu'il était «raciste». Le collectif l'avait pris pour cible une première fois en 2006, avec une série de canulars téléphoniques et d'attaques informatiques contre son site web. Turner avait riposté en publiant les numéros de téléphone des méchants plaisantins, ce qui avait poussé Anonymous à frapper au cœur de son empire radiophonique. Ce dernier avait alors essuyé les assauts de leurs trolls et de leurs hacks. Publié par un Anon peu avant la seconde série de raids, le billet de blog ci-dessous fait foi de l'indéniable sensibilité politique qui marquait l'opération:

> Ceux d'entre vous qui passent leur temps dans les repaires de trolls comme 4chan, 7chan ou YTMND le savent certainement déjà, mais ça vaut la peine de le répéter. En résumé, Hal Turner est un nazi. Un nazi qui a sa propre émission de radio. Malheureusement pour lui, il n'attire pas des masses d'auditeurs, à part les /b/tards et autres trolls fermement déterminés à ruiner sa vie en ligne. Comme on le voit dans le clip extrait de Fox News ci-dessous, où il recommande l'assassinat d'un juge, il ne fait pas franchement pitié[7].

L'opération Chanology se distingue des raids qui l'ont précédée sur un point essentiel: elle est devenue une composante permanente du paysage politique. Dans les semaines et les mois qui ont suivi les premières manifestations, on a continué en effet à dénoncer l'acharnement judiciaire et extrajudiciaire de l'Église de scientologie contre ses opposants et ceux qui osaient divulguer ou faire circuler ses documents internes. «J'suis venu pour le *lulz*; j'suis resté pour la cause, les grandes victoires et encore le *lulz*», m'expliquerait un manifestant lors d'une marche de protestation en Irlande. Mais pourquoi? Et comment les membres d'un groupement aussi chaotique ont-ils pu s'organiser? Le *lulz* pourrait-il survivre à la quête de justice?

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Pourquoi (et comment) nous protestons

Chaque fois que je réfléchis à l'organisation et à la persistance de l'opération Chanology, je suis éblouie par ce que je considère comme un petit miracle de la résistance politique. Des prolongements du trollage tels que la campagne contre Hal Turner avaient certes une dimension politique, mais leur énergie se dissipait généralement au bout de quelques jours ou de quelques semaines. L'opération Chanology, elle, s'est poursuivie, dans un milieu pourtant peu propice à l'organisation politique à long terme. Il nous incombe donc d'examiner la dynamique sociale qui a engendré son succès, en particulier malgré les nombreuses tensions qui l'ont perturbée dès le départ (entre le *lulz* et les finalités morales, par exemple).

Dans un premier temps, le développement d'une volonté politique soutenue a été assuré par l'importante couverture médiatique des manifestations de février 2008. Dès le premier jour, les participants arborant des masques de Guy Fawkes étaient partout dans la presse et les journaux télévisés; par centaines, photos et vidéos des rassemblements locaux étaient partagées sur IRC et les médias sociaux grand public comme Digg, Myspace, Yahoo! Groups et LiveJournal. Aux yeux de beaucoup d'Anons, cette visibilité légitimait l'opération Chanology et Anonymous. Notons que ce type de dynamique, alliant succès et amplification, se répéterait souvent dans l'histoire du collectif.

D'autres facteurs ont aussi joué un rôle important: bien que de nombreux Anons fussent animés par un élan militant (et par le *lulz*, qui ne perdrait jamais son attrait), une bonne partie d'entre eux ont pris part à la campagne parce qu'elle offrait une des rares occasions de rencontrer leurs camarades d'Anonymous en chair et en os. Certains sont restés, tandis que d'autres s'en sont retournés dans les recoins d'internet les plus obscurs afin de blâmer à loisir cette sensibilité politique naissante, traitant parfois leurs semblables de *moralfags* et redoublant d'ardeur dans leur trollage à eux (jusqu'à s'en prendre à l'opération Chanology elle-même pour le *lulz*).

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Prenons l'exemple de la proposition ci-dessous (un appel à extirper Anonymous des mains des *moralfags* en vue de ressusciter la machine de haine d'internet), publiée sur le forum Enturbulation.org, carrefour très fréquenté de l'opération Chanology (maintenant intégré à Why We Protest):

> Confrères et consœurs,
>
> Il y a six mois, nous avons entrepris un djihad pour que notre internet soit exempt de toute *faggotry*. Un appel aux armes a été lancé, et nous y avons répondu par légions. Aujourd'hui, quand nous pensons à cette lutte naïve, il saute aux yeux qu'on nous a volé ce qui nous revient de droit.
>
> Notre nom, nos mèmes et nos efforts ont été détournés par des gens qui n'ont pas compris que notre force découle de notre insensibilité et de notre intransigeance. En temps normal, tout cela devrait aller de soi, mais ceux qui sont restés dans les tranchées pour protéger nos idéaux se trouvent maintenant dans une impasse.
>
> Nous avons besoin de votre aide, et j'implore à genoux les gens qui ont quitté l'opération Chanology d'y revenir et d'en reprendre possession. Ramenez le *lulz*, ramenez la machine de haine, ne vous laissez pas déstabiliser par ces détracteurs acharnés.
>
> Nous avons entrepris cette campagne dans le but de protéger internet de la tyrannie, et, bien que j'admette que des luttes à venir pourraient être plus déterminantes à cet égard, c'était la première d'entre elles. Nous transformons des *newfags* en trolls endurcis et, quand le pouvoir tente de s'approprier ce qui devrait rester accessible et gratuit, nous faisons tout pour l'en empêcher.
>
> Dans les semaines qui viennent, vous verrez de vieux visages arpenter vos canaux, vos forums et vos IRC dans le but de veiller à ce qu'Anonymous conserve ce qui nous appartient. Reprenons possession de Chanology une fois pour toutes, anéantissons tout ce qui s'oppose à nous[8].

Dans les faits, la polarisation entre *moralfags* et amateurs de *lulz* endurcis était (et est toujours) beaucoup moins marquée que ce que laisse entendre

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

cette intervention. Sur les canaux IRC consacrés à l'organisation politique, un groupe minoritaire mais assez actif offrait des conseils techniques sur la lutte politique, tout en martelant l'importance d'agir pour le *lulz*, y compris avec les formes de trollage les plus épouvantables. Parmi ces trolls, un individu se démarquait, nommé (de façon fictive) CPU. Réputé pour ses talents de hacker, il offrait ses conseils sans contrepartie tout en critiquant vertement les *moralfags* et en prônant des formes malveillantes de trollage. Le 16 mars 2008, par exemple, CPU a proposé ce qui suit sur le canal IRC #internethatemachine, un salon de discussion consacré à la critique des *moralfags* (tous les noms ont été modifiés):

> <CPU> Internethatemachine, c'est pour ceux qui n'en peuvent plus des moralfags et des lovefags, non?
> <CPU> On devrait attaquer un forum au hasard pour le lulz. Quelqu'un se souvient des raids sur l'émétophobie?
> <CPU> Je cherche un forum lol.
> <CPU> oh lol http://suicideforum.com/
> <CPU> Le premier qui en pousse un gagne?
> <CPU> Qui se souvient de happy tree friends?:p
> <CPU> On a pourri les forums tous les jours pendant deux semaines
> <CPU> on a fini par avoir emo-corner, mais ça a été long
> <CPU> Trop de monde attaque la même chose en même temps lol
> <CPU> on a fermé leur forum au moins deux fois et défacé la page d'accueil lol
> <CPU> ou alors on pourrait trouver un forum sur l'épilepsie et l'inonder de gifs clignotants ou un truc comme ça
> <XB> http://www.epilepsyforum.org.uk/
> <CPU> go go go
> <CO> omg* il est sur phpbb en plus?:D On va pouvoir se faire plaisir.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> <CPU> On remplace la page d'accueil par un gros truc clignotant?
> <CPU> lol je suis en train de m'ouvrir un compte:D
> <CPU> Si on peut changer la page d'accueil on peut utiliser ça http://www.freetheflash.com/flash/epilepsy-test.php

On ne saura jamais si CPU est passé à l'action, mais quelqu'un l'a fait. Le 22 mars 2012, des trolls ont lancé une des attaques les plus indécentes jamais survenues en envahissant un forum sur l'épilepsie, où ils ont publié des images lumineuses et clignotantes, ce qui a provoqué des crises chez certains de ses membres. Pratiquement tous les reportages ont attribué l'acte à des Anons en lutte contre la Scientologie, ce qui n'était sans doute pas le cas. Sur divers fils de discussions d'*imageboards*, on a mis en cause un autre forum à la réputation douteuse et infesté de trolls: eBaum's World. Même si l'opération Chanology n'était pas derrière le raid, ce dernier a entaché le nom d'Anonymous et enragé certains de ses participants[9].

Notons que, même s'ils jugeaient honteuse l'attaque contre le forum sur l'épilepsie, les nouveaux *moralfags* qu'étaient les croisés anti-Scientologie n'ont pas pour autant désavoué la déviance ou le *lulz*, qui, après tout, étaient partie intégrante de leur culture. L'opération Chanology avait plutôt donné lieu à une variante plus douce du *lulz*, comme avec l'exemple suivant. Chaque année, la ville de New York est le théâtre d'une (assez importante) *flashmob* de zombies, où un millier de cadavres sanguinolents et purulents rampent (ou patinent) dans les rues en grognant. Les organisateurs new-yorkais de Chanology se sont dit que le *lulz* serait bien servi si ces morts-vivants paradaient devant une église de la Scientologie dans le cadre de leur manifestation mensuelle. Les zombies ont accepté l'invitation avec joie. Lentement, ils ont descendu la 46e Rue en criant des obscénités contre la Scientologie devant des manifestants de Chanology morts de rire et visiblement fiers du *lulz* théâtral qu'ils avaient réussi à mettre en scène (lequel convenait pour l'essentiel à un public de tout âge).

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Mais aucun exemple ne peut mieux résumer l'humour carnavalesque des Anons que l'opération Slickpubes (pubis graisseux) de janvier 2009, orchestrée elle aussi par la cellule new-yorkaise de Chanology. Un homme quasi nu enduit de vaseline et couvert de poils pubiens a traversé en courant des bureaux de l'Église de scientologie. Ce geste délirant n'avait pas uniquement pour but de choquer les membres de la secte par un acte de profanation (même si cela faisait indéniablement partie de l'idée), il devait aussi raviver l'esprit du *lulz*, qui, aux yeux de certains membres, était en train de s'amollir. Il fallait veiller à ce que les forces apolliniennes soient éternellement contrebalancées par un soupçon de malice dionysiaque. Plus tard, des membres de Chanology ont commenté l'opération dans un billet de blog publié sur motherfuckery.org, un site conçu pour commémorer leurs origines: «Seuls les termes *lulz* et *u mad* peuvent qualifier ce qui s'est produit dans les mois qui suivirent, alors que les nouvelles de l'opération Slickpubes se répandaient parmi les autres membres de Chanology et d'Anonymous ainsi que dans les hautes sphères de la Scientologie. Ceux qui croyaient Chanology trop sage se sont réjouis[10].»

Au cours de ce processus de politisation d'Anonymous, le *lulz* a souvent été mis en pratique sous une forme facétieuse et dionysiaque, scabreuse et risquée. Les Anons faisaient à la fois rire et grimacer, tout en proposant une politique de la subversion. Mais ce choix n'a pas été sans conséquence. Dans le cas de l'opération Slickpubes, le *streaker* graisseux s'est fait arrêter pour ses clowneries. L'incident a aussi amené la police de New York à entreprendre une surveillance discrète d'Anonymous (un baptême incontournable pour tout nouveau groupe politique – et quoi de mieux que des poils pubiens pour attirer les forces de l'ordre?)[11]. Le Sage barbu avait peut-être dompté Anonymous, mais n'avait pas complètement éradiqué sa malice.

La volonté d'Anonymous de faire des ravages pour le *lulz* et la liberté d'expression (par opposition à la malhonnêteté et aux duperies de la Scientologie) rappelle les «bandits sociaux» européens du XIX^{e} siècle, décrits par l'historien Eric Hobsbawn dans *Les primitifs de la révolte dans l'Europe moderne*, paru en 1959. Membres de la mafia, de sociétés secrètes,

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

de sectes religieuses, de gangs urbains ou de bandes de hors-la-loi, ces bandits sont essentiellement des voyous, mais, selon Hobsbawn, ils sont porteurs d'un vague esprit révolutionnaire: ils redistribuent généralement une partie de leur butin aux pauvres, qu'ils protègent en outre contre d'autres bandits. L'historien les qualifie de «populations prépolitiques qui n'ont pas encore trouvé une dialectique pour exprimer leurs aspirations[12]». Depuis le lancement de l'opération Chanology, les Anons, eux, s'activent de façon remarquable pour trouver cette dialectique.

Leurs frasques contrastent cependant avec le propos moralisateurs de Hobsbawn selon qui les bandits ne peuvent devenir des acteurs politiques dignes de ce nom qu'en renonçant à leurs méthodes barbares et en adhérant aux formes conventionnelles d'exercice du pouvoir. Pour Hobsbawn, «le bandit est impuissant devant les forces de la société nouvelle qu'il ne peut comprendre. Au mieux, il peut la combattre et essayer de la détruire». C'est pourquoi il est «souvent plus destructeur et cruel que ne le voudrait sa légende[13]». Les bandits numériques d'aujourd'hui, eux, comprennent les forces de la destruction créative, qu'ils utilisent consciemment à des fins politiques.

Le *lulz* occupe chez eux une place importante, mais pas la principale. Chanology n'a rien d'une horde chaotique de fous furieux. Même s'ils émanent d'un milieu souvent malsain, marqué par des conflits entre groupes ou individus, ses membres ont su bâtir une organisation solide, à laquelle certains d'entre eux consacrent énormément de temps. Prenons par exemple la programmation qu'a demandé la création du très populaire forum Why We Protest, attribuable en grande partie au jeune geek français Ravel. Pour lui, il était tout naturel de prendre part à l'opération Chanology, car il avait «quelques années de mauvais tours derrière la cravate et une forte affinité avec les cultures du hacking et de la liberté d'expression. Quand j'ai entendu l'appel à l'action, j'y ai répondu sans attendre[14]». Il y consacrerait les six années suivantes, et ce n'est pas fini.

Le projet de forum est né sur le canal IRC #website. Ravel (connu sous le pseudo de Sue) était insatisfait des modèles proposés. En bon hacker, il a entrepris de coder les logiciels à sa façon, aidé de deux autres

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

programmeurs. Impressionnés par son travail, les membres de marblecake l'ont recruté:

> On m'a invité à devenir membre du formidablement infâme collectif marblecake. [...] À ce jour, il s'agit du groupe le mieux organisé avec lequel j'aie collaboré en ligne. Je n'exagère rien en disant que le gros de ses participants passait plus de soixante-dix heures par semaine à élaborer des projets multimédias, à planifier des opérations, à faire des coms et du *brainstorming*. Il s'agissait à la fois d'un laboratoire d'idées et d'un studio de production. Nous avions des réunions presque tous les jours; nous y procédions à des évaluations, y prenions des notes, etc.[15].

«C'est quoi, ce foutu marblecake?»: premiers réquisitoires contre le nouvel Anonymous

Étant donné la part importante des Anons qui se consacrait désormais au hacking politique (avec son infrastructure technique de canaux, ses réunions mensuelles et sa panoplie naissante de mèmes et d'objets propres à un Anonymous militant, tel le masque de Guy Fawkes), ce n'était qu'une question de temps avant que des lignes de fracture ne viennent lézarder l'identité du collectif. L'homéostasie n'est pas exactement le mode d'être de prédilection d'Anonymous – certainement pas avant l'opération Chanology, et assurément pas après.

Attardons-nous un moment sur le fait que Ravel qualifie marblecake de «groupe le mieux organisé avec lequel j'aie collaboré en ligne». De l'avis général, marblecake faisait montre d'une efficacité redoutable dans la propagande – rédaction de communiqués de presse, négociation entre cellules de différentes villes et proposition de thèmes pour les manifestations mensuelles. Pour de nombreux participants et observateurs, son succès était notamment attribuable à une organisatrice chevronnée connue sous le pseudo de darr. Un Anon me l'a décrite comme une femme

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

«décidée et fière, bienveillante et compréhensive», des qualités qu'il juge indispensables aux réalisations de marblecake.

Mais darr commettrait l'erreur de faire aboutir une proposition impopulaire. En vue de la manifestation de mai 2008, marblecake avait suggéré le thème «opération Psychout» (intimidation), qui aurait consisté à révéler les violations des droits de la personne commises par la Scientologie en matière de psychiatrie. L'idée «s'est heurté à une grande opposition», selon un membre actif. Peu après, marblecake a planté le dernier clou de son cercueil (du moins sous la forme qu'il avait alors) en tentant de «faire passer la proposition en force», ce qui a incité des membres de Chanology à «remettre darr à sa place» parce que cette «*leaderfag* ambitieuse et assoiffée de pouvoir» avait une trop grande gueule à leur goût. Les trolls, en particulier, l'ont attaquée sur ses points faibles en divulguant certaines données privées et en répandant des rumeurs à son endroit. Elle a abandonné l'opération, et on ne l'a plus revue depuis.

Les contours de marblecake étaient indistincts. Au moment de partir de leur côté en janvier 2008, ses huit Anons fondateurs avaient laissé une notification permanente sur le canal #press: «Tu veux être dans le feu de l'action? Branche-toi par SSL et ne fais pas le *faggot* ;D — Sujet créé par darr le 16/02/2008.» Ceux et celles qui étaient séduits par ce message sibyllin pouvaient chercher à en savoir plus auprès d'un *oldfag* (un membre fondateur), qui leur indiquerait comment établir une connexion par protocole sécurisé SSL. On leur expliquait aussi qu'ils et elles devaient s'attendre à donner beaucoup de leur temps. C'est ainsi que marblecake a pu totaliser 25 membres. La notification finirait par être retirée, si bien que l'expansion du sous-groupe prendrait fin et que les néophytes ignoreraient son existence.

Trois mois après l'expulsion de darr, quelqu'un a publié ce message sur Why We Protest: «C'est quoi, ce foutu marblecake?» La réponse qu'il a obtenu a révélé l'existence de ce projet à demi secret à un groupe beaucoup plus large d'Anons, dont bon nombre découvraient ainsi que l'opération Chanology était divisée en multiples factions:

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> Je fais partie de marblecake et je n'ai aucune envie d'être un *leaderfag*.
>
> Je serai heureux de répondre aux questions.
>
> En bref, c'est/c'était un petit groupe de réflexion qui produisait du contenu multimédia de façon anonyme et secrète. En voyant les choses du bon côté, on pourrait dire que le groupe a été «victime de son succès»: il a produit assez de contenu ayant eu un impact pour juger bon de rester dans le secret absolu... mais aussi pour que les autres membres d'Anonymous soient conscients (à divers degrés) de l'existence d'une cabale d'Anons cherchant à trafiquer en coulisse.
>
> Le mauvais côté est que... il s'agit d'une cabale d'Anons cherchant à trafiquer en coulisse. Et il faut souligner qu'ils ont eu très vite la grosse tête. C'est eux qui ont produit le premier «message à la Scientologie» (bien avant que j'y sois). Ils étaient dirigés par darr, qui faisait chier les mauvaises personnes, avait une attitude de merde et tolérait en général mal la critique.
>
> [...]
>
> Au sujet des factions, il y a marblecake, enturbmods (sic), OCMB et les canaux #enturbulation (en plus des cellules de chaque ville et probablement d'autres sous-groupes dont j'ignore tout). marblecake et enturbmods se sont battus l'un contre l'autre. #enturbulation (précisément Tuesday et WB) a combattu marblecake. OCMB fait souvent des histoires à propos d'enturbulation. #enturbulation, en général, déteste marblecake. Ces luttes intestines sont débiles; bien des gens ont été impliqués dans plusieurs de ces groupes. Et personne ne devrait se sentir «exclu» de ne pas en faire partie, car ces groupes sont essentiellement les concierges des *vrais* Anons, ceux qui sont dans les rues à distribuer des tracts et à manifester[16].

S'en est suivi un fil de discussion interminable, plein de rancœur. Certaines interventions étaient cinglantes, y compris de la part de membres et d'ex-membres de la cabale. Après tout ce tintouin, marblecake a été rayé de la carte pour un certain temps avant d'entreprendre ce qu'un Anon a qualifié

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

de «refondation». Ses membres allaient désormais faire preuve d'une certaine transparence dans leur rôle de «chorégraphes», pour emprunter l'expression utilisée par Paolo Gerbaudo pour décrire un mode de direction propre à la plupart des mouvements de contestation du monde en 2011[17].

La révélation de l'existence de marblecake a montré qu'une simple polarisation entre dirigeants et exécutants ne pouvait rendre compte de la dynamique organisationnelle complexe d'un milieu très attaché à son mode de fonctionnement décentralisé. Anonymous n'est pas un front uni, mais plutôt une hydre constituée d'une multitude de réseaux différents. Même dans le cadre d'une opération précise, on voit souvent des groupes de travail s'opposer les uns aux autres, sans parler des conflits plus généraux qui mettent aux prises les divers nœuds d'Anonymous. Néanmoins, si les Anons ne sont pas toujours d'accord sur ce qui peut être entrepris au nom d'Anonymous, ils ont tendance à respecter le fait que tout un chacun peut se réclamer de l'appellation. Le masque, devenu l'emblème du collectif, joue le rôle d'un flambeau éternel symbolisant le principe d'égalité, en dépit des divisions et des inégalités internes. Évidemment, malgré l'absence d'une hiérarchie stable ou d'un centre décisionnel précis, certains Anons sont plus actifs et influents que d'autres, ne serait-ce que pour de brefs laps de temps. Anonymous applique une variante particulière de ce que les geeks appellent «action-cratie», où ceux et celles qui sont motivés (ou très disponibles) développent son architecture en réseau en offrant leur temps, leur énergie et leur attention aux opérations existantes, ou en démarrant leurs propres projets, plus conformes à leurs idéaux et à leurs principes.

La reconnaissance ou non de l'existence d'une élite informelle dans un mouvement est une question importante. Elle est liée à un autre problème qui mine de nombreux mouvements sociaux: comment des groupes existants, où tend à se développer un esprit de clan, peuvent-ils rester assez ouverts pour continuer d'accueillir des nouveaux venus? Si les membres ignorent les rapports de force qui s'exercent entre eux, le collectif peut facilement sombrer dans la «tyrannie de l'absence de structure», une situation où l'idéologie de la décentralisation devient une formule creuse qui masque l'existence d'une hiérarchie[18].

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

À la suite de la vive controverse ayant fait rage sur Why We Protest, de nombreux Anons ont néanmoins fini par admettre que l'élite informelle de marblecake avait accompli un travail d'organisation impressionnant et précieux, sur le net comme dans les groupements locaux. Mais la nécessité d'une plus grande transparence a fait consensus.

«La Scientologie ne peut plus rien contre nous; c'est terminé»

En 2014, l'opération Chanology n'est plus que l'ombre de ce qu'elle était. Les manifestations mensuelles n'attirent désormais que ses militants les plus résolus et des foules rachitiques dans une poignée de villes (telles Dublin, Düsseldorf, Hambourg et New York). Cette situation ne témoigne toutefois pas d'un échec, mais bien d'une réussite. Bien que l'opération ne soit pas venue à bout de l'Église de scientologie, elle a changé la donne à un point tel que les opposants à la secte peuvent maintenant s'exprimer haut et fort sans crainte de représailles. Les scientologues n'ont plus l'avantage.

C'est ce que m'ont fait comprendre de nombreux ex-scientologues lors d'un congrès intitulé Dublin Offlines, le 30 juin 2012. Cela faisait plus de quatre ans qu'un improbable élixir s'était mis à fermenter à partir d'un mélange hétéroclite d'anciens membres de la secte, d'opposants à la Scientologie et de geeks arrogants. L'occasion me semblait idéale pour faire le point sur la portée historique de l'opération.

La rencontre avait lieu au Teacher's Club de Dublin (également connu sous le nom de Club na Múinteoirí), qui occupe un immeuble de style georgien de quatre étages offrant un abri douillet contre l'incessante bruine irlandaise. Environ 70 personnes étaient présentes, dont une bonne partie portait des masques de Guy Fawkes. Fidèles à la théâtralité qu'ils affichaient lors des manifestations, certains Anons français arboraient avec panache des tenues de cirque ou de pantomime. Deux d'entre eux étaient même déguisés en farfadets géants. Mon préféré était celui en costume de vache.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Parmi les conférenciers se trouvaient d'anciens scientologues, dont certains avaient fait partie de la Sea Org (l'autorité suprême de l'Église), Gerry Armstrong (ex-secrétaire personnel de L. Ron Hubbard), Jamie DeWolf (arrière-petit-fils de Hubbard), quelques professeurs (dont moi) et une poignée de personnes ayant perdu des proches aux mains de la secte. L'événement était animé par Pete Griffiths, ancien directeur général de la mission de Kendal, une ville du comté de Cumbrie en Angleterre; son flamboyant costume gris argenté convenait parfaitement à sa personnalité pleine d'entrain.

Comme j'étais hébergée à l'autre bout de la ville, je suis arrivée en retard au congrès, qui battait déjà son plein. Je me suis avancée sur la pointe des pieds en saluant de la main les quelques Dublinois que j'avais connus lors d'un séjour précédent. Je me sentais bien, quoiqu'en manque de caféine. Plus tard, au terme de cette journée ponctuée de nombreux exposés poignants, je me sentirais émotionnellement vidée. Les ex-scientologues ont en effet témoigné du pouvoir d'une secte capable de briser la vie de ses membres comme de ceux qui osent la quitter. L'Église de scientologie oblige ses nouvelles recrues à rompre tous liens avec leurs parents ou amis qui s'opposent à leur adhésion (et ils sont nombreux). Parce qu'il ne reste plus grand-chose de leur réseau social, les membres qui fuient l'organisation vivent souvent un cauchemar logistique. Lorsqu'un membre annonce publiquement sa rupture, il devient une «cible légitime», ce qui signifie qu'il «peut voir sa propriété confisquée ou peut être blessé par tous les moyens et par tout scientologue sans que ce dernier encoure le moindre reproche de la part de la Scientologie. On peut le tromper, le poursuivre en justice, lui mentir ou le détruire[19]».

Le témoignage de Tory Christman est sorti du lot. Au moment de quitter la secte, le 20 juillet 2000, elle y avait passé trente-et-un ans, au cours desquelles elle avait parfait ses talents d'oratrice en tant que responsable des communications. Sûre d'elle, Christman est une femme éloquente, inspirante et pleine d'esprit; le jour du congrès, avec ses lunettes rectangulaires et son tailleur bleu clair, elle était rayonnante. Pendant trente minutes, elle s'est adressée à une salle pleine. Elle a raconté son arrivée

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

dans l'Église et les expériences les plus pénibles qu'elle y a vécues (dont l'épisode où l'on a tenté de la dissuader de prendre ses médicaments contre l'épilepsie). Elle a aussi donné un aperçu des méthodes employées par la secte pour laver le cerveau de ses recrues («une prise de contrôle progressive de l'esprit») et présenté la théologie scientologique, enseignée dans des cours offerts à prix d'or («la lecture de "Comment faire en sorte que la Scientologie continue à fonctionner" est au programme de chacun des cours»). Vers la fin de sa conférence, elle a raconté sa fuite désespérée («on m'a pourchassée d'un bout à l'autre du pays»), en insistant bien sur le fait ironique que l'Église de scientologie «vous vend la liberté, mais vous réduit en esclavage».

Christman a pris soin de saluer le rôle joué par Anonymous: «Nous pouvons maintenant tous nous permettre [d'en parler en public] grâce (a) à internet, (b) aux opposants d'avant Anonymous et (c) à Anonymous. D'accord? Anonymous a complètement changé la donne. Pour de bon. Nous le savons tous.» Elle n'en a pas moins applaudi le courage de la génération antérieure d'opposants, qui comptait quelques représentants dans la salle. Ceux-ci avaient agi à visage découvert à une époque où les déserteurs étaient rares et où la Scientologie avait la capacité de détruire la vie de ses adversaires en les attaquant en toute impunité. «Nous ne serions pas en train de parler d'Anonymous si ces opposants-là ne les avaient pas précédés.»

Elle a ensuite lancé une phrase qui a résonné dans toute la salle, touchant chaque participant droit au cœur: «La Scientologie ne peut plus rien contre nous; c'est terminé.» Aux ex-membres de la secte, ces mots étaient à la fois source de soulagement et de réjouissance. Quant aux Anons, dont certains s'étaient liés d'amitié avec des déserteurs, ils ressentaient sans doute une grande fierté: nul délice ne surpasse celui d'une victoire politique, et l'opération Chanology avait accompli l'improbable: le groupe était parvenu à ébranler une organisation qui semblait toute-puissante, imperméable à la critique et au-dessus des lois.

Mais le plus admirable, c'est qu'une lutte politique d'abord ponctuelle contre un ennemi bien défini s'était élargie pour se muer en un projet

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

politique global et diversifié, dont le rayonnement s'était étendu à la planète entière: *Anonymous Everywhere*. Penchons-nous maintenant sur les événements improbables qui, de façon surprenante, ont propulsé Anonymous sur le devant de la scène.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Chapitre 3

Les armes des geeks

WikiLeaks: la corne d'abondance

JUILLET 2010. Je participe à un forum intitulé Hackers on Planet Earth (HOPE), qui se tient tous les deux ans à New York dans un lieu charmant et chargé d'histoire, l'hôtel Pennsylvania (qui, à l'instar de l'hôtel de *The Shining*, est sinistrement vétuste). Une fois ma conférence terminée, je me laisse imprégner de l'ambiance vraiment particulière de cet événement – saturée de politique, mais lourde de drame, d'intrigue et de suspense. L'atmosphère électrique qui règne à HOPE n'est pas attribuable à Anonymous. Car même si on considère déjà le collectif comme une curiosité politique, il est encore un acteur mineur sur le plan géopolitique. Certains de ses militants ont commencé à s'investir dans de nouvelles causes (tel le soulèvement postélectoral de 2009 en Iran), mais l'opération Chanology reste son principal cheval de bataille, avec ses inlassables dénonciations des violations des droits de la personne commises par l'Église de scientologie et ses manifestations mensuelles dans des villes d'Amérique du Nord, d'Australie, d'Europe et d'autres régions du monde. Beaucoup de trolls se réclament encore d'Anonymous, mais leur mouvance vouée au «salopage ultracoordonné sur internet» connaît un indéniable déclin.

Non. L'enjeu qui donnera le ton au forum est lié à un autre acteur: WikiLeaks, nouvel outil de prédilection des lanceurs d'alerte. Plus

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

précisément, l'intérêt portera sur la divulgation d'un trésor de documents et de vidéos par le jeune soldat Bradley Manning (devenu par la suite Chelsea Manning), révélé à la face du monde par le site web WikiLeaks. Créé en 2006, ce dernier repose sur un concept simple qui consiste à offrir une plateforme à la fois sûre et centralisée pour déposer les documents faisant l'objet d'une fuite. En service depuis quelques années déjà à ce moment-là, le site avait rendu possibles d'innombrables fuites, mais à ce stade il n'avait pas encore suscité l'intérêt de grandes institutions médiatiques telles que le *New York Times.* Les informations révélées étaient pourtant loin d'être futiles. Certaines d'entre elles (comme le déversement de déchets toxiques au large de la Côte d'Ivoire par la multinationale Trafigura) étaient proprement scandaleuses, mais elles n'en avaient pas moins été scandaleusement ignorées des grands médias. Certains d'entre eux s'y étaient tout de même risqués, non sans difficultés. Le gouvernement britannique, par exemple, avait empêché le quotidien de gauche *The Guardian* de rendre publique l'affaire Trafigura. «*The Guardian* s'est aussi vu interdire d'informer ses lecteurs des raisons pour lesquelles on lui a interdit, pour la première fois de son histoire, de couvrir un débat parlementaire. Ces obstacles juridiques dont nous ne pouvons faire état découlent d'une procédure dont nous sommes tenus de taire la nature, engagée au nom d'un client dont le nom doit être tenu secret», écrivait un de ses directeurs de rédaction[1].

En avril 2010, la stratégie de communication de WikiLeaks a connu une transformation spectaculaire. Lorsqu'ils ont publié des séquences vidéo d'un bombardement de Bagdad sous le titre «Meurtres collatéraux», en effet, les responsables du site n'ont rien laissé au hasard: un vidéo-montage soutenu d'un commentaire éditorial efficace venait rendre encore plus choquante cette nouvelle qui l'était déjà. Qui plus est, après avoir cultivé le mystère autour de sa personne, le hacker australien et fondateur de WikiLeaks Julian Assange a rompu avec cette stratégie en organisant une conférence de presse à Washington suivie d'une tournée très médiatisée.

La réaction de la presse et du public a été tout bonnement explosive. Selon le spécialiste des médias Christian Christensen, si cette vidéo est

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

«une des réussites les plus célèbres et les plus largement reconnues du projet WikiLeaks», c'est parce qu'elle «fournit les preuves visuelles d'un flagrant abus de pouvoir de l'État et des forces armées[2]». Les séquences en noir et blanc montrent le point de vue d'un soldat qui, à bord d'un hélicoptère Apache, massacre des civils en périphérie de Bagdad. Tournée en 2007, la vidéo souleva bien des questions. Pourquoi ne l'avait-on jamais vue auparavant? Parmi les victimes de l'assaut se trouvaient deux journalistes de Reuters. Se doutant qu'un acte criminel avait été commis (et ses soupçons étaient loin d'être infondés), l'agence de presse avait, dans les années subséquentes, tenté de mettre la main sur le document par des requêtes en vertu du Freedom of Information Act (loi sur le libre accès à l'information). Cette vidéo, en outre, venait rappeler à quel point les grands médias s'étaient écartés de leur mission d'information dès lors qu'ils avaient renoncé au journalisme de guerre direct (et macabre) qu'ils avaient pratiqué dans les dernières années de la guerre du Vietnam.

Mais, par-dessus tout, dans cette vidéo, c'est le ton de voix détaché des pilotes, dont le calme frise la psychose, qui a suscité le plus grand dégoût. On entend par exemple un membre de l'équipage se mettre à rire lorsqu'il réalise qu'une petite fille fait partie des victimes: «Ils n'avaient qu'à pas ramener leurs enfants à la guerre», lance-t-il avec désinvolture.

Comme on le sait, Chelsea Manning déciderait de divulguer la vidéo avec d'autres documents d'importance capitale, puis se ferait moucharder par un hacker appelé Adrian Lamo. Le 22 mai 2010, lors d'une séance de chat, elle lui a en effet confessé avoir transmis à WikiLeaks les séquences de «Meurtres collatéraux», cela après que Lamo eut gagné sa confiance en se présentant sous une fausse identité. «Je suis journaliste et prêtre. Vous pouvez retenir l'un ou l'autre de ces titres et considérer ce que vous allez me dire comme une confession ou comme une interview (qui ne sera jamais publiée), tout en jouissant d'un minimum de protection juridique[3].»

C'est ainsi que Manning a vidé son sac à quelqu'un qu'elle n'avait jamais rencontré et dont les chances qu'il soit vraiment journaliste et prêtre étaient, au mieux, ténues[4]. Lamo a transmis la conversation au Federal Bureau of Investigation (FBI) et au magazine *Wired*. Le FBI a arrêté

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Manning, qui a fini par avouer qu'elle avait communiqué non seulement les séquences de «Meurtres collatéraux», mais aussi des câbles diplomatiques, que WikiLeaks divulguerait au cours des deux années suivantes. Après avoir passé un an en isolement, Manning a été condamnée à trente-cinq ans de prison par un juge militaire. Elle est aujourd'hui incarcérée à Fort Leavenworth[5].

Au forum HOPE de 2010, la tension est palpable. Une rumeur circule voulant que Julian Assange prononce le discours d'ouverture. À la dernière minute, ce n'est pas Assange qui monte sur scène, mais le hacker américain Jacob Appelbaum. Pendant son discours – captivant –, il révèle à tous (y compris aux inévitables agents fédéraux présents dans la salle) qu'il est associé à l'organisation assiégée. C'est courageux de sa part, vu les tentatives de musellement, les poursuites et l'intimidation dont WikiLeaks fait déjà l'objet. Selon Appelbaum, WikiLeaks s'inscrit historiquement dans ce qu'il est maintenant convenu d'appeler le «cinquième pouvoir», constitué des hackers, des lanceurs d'alerte, des journalistes indépendants et des blogueurs qui exercent la fonction critique autrefois dévolue au «quatrième pouvoir» que sont les grands médias. «Quand les médias sont bâillonnés, nous refusons d'être bâillonnés, nous refusons de garder le silence», lance-t-il, ce qui lui vaut un tonnerre d'applaudissements. (C'est le *New York Times* qui, ces dix dernières années, a offert l'exemple le plus frappant de ce silence des médias lorsqu'il a refusé, à la demande du gouvernement, de publier un article sur les pratiques illégales d'écoute électronique de la National Security Agency (NSA). Le quotidien a fini par publier l'article, mais uniquement parce que son auteur, James Risen, s'apprêtait à le priver de son exclusivité en faisant paraître un livre sur le sujet. Ironie du sort, l'article a remporté un prix Pulitzer.)

À HOPE, les hackers politisés et défenseurs de la transparence qui interviennent ne parlent pas seulement de WikiLeaks, de «Meurtres collatéraux» et de Manning: il est aussi beaucoup question de Lamo, le hacker traître. Son nom est sur toutes les lèvres pour une raison bien simple: comme les autres participants, il est lui-même un hacker – sans parler du fait qu'il est présent à la conférence! Les gens sont vraiment en rogne.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Pendant son discours sur WikiLeaks, Applebaum promet de ne pas parler de Lamo, mais, en même temps qu'il prononce ces mots, il ouvre sa chemise et dévoile un t-shirt sur lequel est inscrit «Non à la délation», déchaînant la foule. Des tracts arborant le visage de Lamo sont lancés dans la salle: «RECHERCHÉ. Mort ou vif. Pour être un salopard de déchet, un ignoble rat.»

Alors que j'ai le regard fixé sur le tract, un ami hacker surgit pour me saluer. Tout en grimaçant son dégoût pour Lamo, il m'explique qu'Assange, «c'est du solide» – éloge rare de la part d'un hacker. Il l'a connu dans les années 1990, alors que l'underground hacker était au maximum de sa puissance et hantait les réseaux en toute liberté, à l'abri d'une répression qu'il ne commencerait à subir qu'à la fin de la décennie. Au mépris de la loi, ses membres exploraient les réseaux privés et les systèmes informatiques; et leur motivation n'était pas le profit ni de mauvaises intentions, mais plutôt une curiosité insatiable, un désir de comprendre le fonctionnement des choses. Même si la transgression était elle-même source de satisfaction, certains de ces hackers menaient des activités ouvertement militantes. Julian Assange était l'un d'eux. Très consciencieux, il allait jusqu'à rédiger des manifestes pour justifier ses actions. Assange faisait partie d'un groupuscule appelé International Subversives, qui respectait le crédo suivant: «N'endommage pas les systèmes informatiques dans lesquels tu t'introduis (et ne les fais pas planter); ne modifie aucune information qu'ils contiennent (à part leurs journaux, d'où tu dois effacer tes traces); diffuse l'information[6].»

Alors que nous achevons notre conversation sur Assange tombe une nouvelle formidable: le principal organisateur du forum HOPE, Eric Corley (plus connu sous son pseudo de hacker Emmanuel Goldstein), vient d'annoncer qu'il y aura un panel improvisé sur le thème de la délation et des délateurs, auquel prendra part nul autre que Lamo. Ce dernier ira s'asseoir aux côtés de *phreakers* et de hackers parmi les plus célèbres de tous les temps: Bernie S., Mark Abene (Phiber Optik) et Kevin Mitnick, qui, devant l'adversité judiciaire, se sont gardés de «collaborer» avec les autorités, un silence qui leur a valu de lourdes peines d'emprisonnement.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

J’ai fréquenté des rassemblements de hackers pendant de nombreuses années, et ce panel reste le plus extraordinaire de tous ceux auxquels j’ai assisté. Imaginez 2 600 hackers assis devant un homme seul, traître honni de tous, qui les lorgne depuis la scène et tente de justifier ses actes.

Une assemblée de hackers sur la délation devant le mouchard le plus détesté de tous les temps

Les panélistes commenceront par raconter quelques-uns de leurs exploits en décrivant comme ils avaient peur de se faire prendre et d’être trahis par des camarades. Goldstein, qui est le premier à prendre la parole, rappelle une évidence que je serai à même de vérifier ultérieurement avec Anonymous: quand les policiers débarquent chez quelqu’un (souvent à l’aube, en tambourinant à la porte, armes au poing), «il panique. [...] Les autorités comptent là-dessus pour obtenir le plus d’informations possible, pour amener le prévenu à les renseigner sur d’autres suspects potentiels».

Arrive Lamo, qui monte sur scène et se dirige lentement vers son siège. Lorsqu’il cligne des yeux, qu’il a profondément cernés, il le fait très lentement, avec grande difficulté, comme s’il devait chaque fois forcer ses paupières à se baisser. Il ne semble pas particulièrement nerveux – plutôt complètement abruti par les médicaments. Cet ancien *black hat** (chapeau noir) respecté entreprend de légitimer ses gestes et il est fascinant de l’écouter. C’est au nom de la défense nationale, explique-t-il, qu’il s’est senti «obligé» de transmettre ses échanges aux autorités. Bernie S., qui veut plus de détails, l’interrompt avec respect: «En quoi considériez-vous que la population était en danger?» Lamo lui fait cette réponse pour le moins décousue: «Le département d’État participe à un certain nombre d’opérations de renseignement dans le monde, euh, il n’est pas censé le faire, mais il veille aux intérêts des Américains.» Ses propos provoquent des sifflements dans la salle; un spectateur crie: «Les activités du département d’État mettent d’autres gens en danger!»

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Goldstein sent que l'auditoire réprime des envies de lynchage, qu'il est près d'affûter ses fourches et d'allumer ses torches pour chasser Lamo de la ville. Il parvient à ramener un certain calme en déclarant «Votre tour de parole viendra», mais pas avant que Phiber Optik ne ricane: «Ne vous inquiétez pas, nous allons juste sortir nos arcs et nos flèches.» Cette touche d'humour fait baisser la pression, mais l'atmosphère redevient rapidement tendue (et le restera jusqu'à la fin). Invariablement, les tentatives de Lamo de justifier ses actes sont accueillies par des huées furieuses. Lorsqu'il se porte à la défense du gouvernement et qualifie son rapport avec les agents d'«étonnamment agréable», même Goldstein ne peut se retenir et lui coupe la parole avant la période de questions pour lui demander ce qu'il ressent devant la possibilité que Manning passe le reste de ses jours en prison (un spectateur hurle aussi «Torture!»). Du tac au tac, Lamo réplique d'une voix atone: «Nous n'infligeons pas cela à nos citoyens.» C'est à ce moment-là que retentissent les huées et les sifflements les plus forts. «Guantánamo!» crie quelqu'un. Quoi qu'il dise, Lamo creuse manifestement sa tombe, et presque toute la salle semble prête à le couvrir de terre.

Sur le moment, malgré l'intérêt que je portais au débat, je n'ai pas vu le rapport avec mon projet de recherche sur Anonymous. WikiLeaks et Anonymous vivaient alors sur deux planètes différentes (même s'ils appartenaient à la même galaxie de geeks en raison de leurs luttes respectives contre la censure et contre la Scientologie[7]). Ce n'est qu'un an plus tard, soit le 4 juillet 2011, que j'ai eu ma toute première conversation privée par Internet Relay Chat (IRC) avec le plus célèbre mouchard d'Anonymous, Hector Monsegur, connu jusque-là sous le pseudo de Sabu. À ce moment-là, il s'était déjà fait arrêter et collaborait en catimini avec le FBI – ce que nous étions nombreux à ignorer malgré un faisceau d'indices évidents. Grâce à son charisme – et aussi en usant de ses talents de manipulateur pour détourner les soupçons sur autrui –, Monsegur avait en effet réussi à ce que personne ne saisisse les allusions qu'il avait pourtant laissées en toutes lettres quelques mois après son arrestation secrète: «Restez vous-mêmes», avait-il écrit sur Reddit. «Si vous faites partie d'une équipe, assurez la sécurité de vos opérations 24 h sur 24. Des amis

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

essaieront de vous abattre s'ils n'ont pas le choix[8].» N'y avait-il pas là comme un écho de la leçon apprise par Manning l'année précédente?

Quoi qu'il en soit, ces soucis avec les délateurs ne représentent que la plus ténue des connexions alors balbutiantes entre WikiLeaks et Anonymous (nous y reviendrons dans le chapitre 4). Une association bien plus directe apparaît dès lors qu'on observe la trajectoire d'AnonOps.

Attaques par saturation à une date fixée au départ

AnonOps voit le jour en 2010, quelques mois à peine après le forum HOPE. D'abord simple nœud d'Anonymous, le projet évoluera vers un réseau IRC à part entière, qui prendra le monde d'assaut avec ses expériences (à proprement parler, car le groupe ne se donnera la peine d'y réfléchir que bien plus tard) impliquant tout un lot de tactiques d'action politique directe. Dont une bonne partie seront carrément illégales, si bien qu'elles attireront vite l'attention du FBI.

Les trajectoires d'AnonOps et de WikiLeaks vont se croiser en décembre 2010, mais ces deux organisations sont à cent lieues l'une de l'autre en ce qui concerne leur fonctionnement. WikiLeaks est l'œuvre d'une vie, sculptée avec le plus grand soin. Son fondateur et porte-parole Julian Assange en contrôle la plupart des aspects (trop étroitement selon certains). L'identité et la personnalité d'Assange sont d'ailleurs intimement associées au nom de WikiLeaks: quand sa réputation a été souillée, toute l'organisation a été éclaboussée. En revanche, comme pour l'opération Chanology, c'est un concours de circonstances fortuites qui est à l'origine d'AnonOps: divers événements, suscitant l'attention des médias, ont permis de contribuer à son essor fulgurant. Voilà qui rappelle une fois de plus à quel point ces *tricksters* que sont les Anons sont toujours prêts à tirer parti des imprévus et gagnent parfois à agir sur un coup de tête.

L'origine d'AnonOps remonte à la fin août 2010, environ deux ans et demi après que des hackers eurent adopté le nom d'Anonymous pour s'aventurer dans l'univers du militantisme. À ce moment-là, les membres

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

de l'opération Chanology ont déjà organisé des manifestations, noué des alliances et des amitiés solides avec d'ex-scientologues, pris part au soulèvement postélectoral de 2009 en Iran et étendu leurs activités à d'autres domaines du militantisme sur le net. En février 2010, en réaction à un projet de règlement du ministre des Télécommunications australien qui visait à filtrer la pornographie sur internet, des Anons lancent l'opération Titstorm (tempête de nichons), dans le cadre de laquelle ils saturent les serveurs de l'État en les inondant de requêtes. Cette campagne, qui s'inscrit dans l'opération Freedom Movement, est un signe annonciateur de ce qui va suivre.

Le 5 juillet de la même année, soit cinq jours avant le forum HOPE, des Anons relancent l'opération Freedom Movement sous le nom d'Internet Freedom Movement (IFM)[9]. De concert avec le reste du milieu geek, les membres de l'IFM envisagent une campagne de protestation contre l'Accord commercial anticontrefaçon (ACTA). L'ACTA vise notamment la mise en place d'une réglementation d'envergure qui criminaliserait toute violation du droit d'auteur et inciterait les fournisseurs d'accès internet à pister et à surveiller leurs clients en vue d'établir leur profil. Le projet d'accord suscite une opposition acharnée. Pratiquement tous les groupes qui luttent pour un internet plus accessible (dont l'Electronic Frontier Foundation, la Free Software Foundation, Public Knowledge et La Quadrature du Net) critiquent le secret dans lequel le document a été négocié et s'opposent catégoriquement à son adoption.

L'IFM souhaite faire pression sur les élus et sensibiliser le public à l'aide de documents divers et de sites web. Ses membres ont créé un forum de discussion spécialement pour la campagne, #antiactaplanning, sur le serveur IRC OccultusTerra. Fin août 2010, un Anon s'exprimant sous le nom de golum (qui n'est pas son pseudo habituel) se connecte au forum et y annonce hardiment son intention de faire avancer le dossier en menant une attaque par saturation contre le site du bureau du représentant au commerce des États-Unis, ustr.gov, le 19 septembre à 21 heures HNE. Parce que l'ACTA est un accord commercial proposé par les États-Unis et que le bureau du représentant au commerce a le pouvoir d'infliger des sanctions

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

aux États qui contreviennent aux accords commerciaux, le choix de cette cible va de soi.

L'annonce de golum suscite des questionnements chez beaucoup de participants. En premier lieu, l'opération Chanology a établi un précédent politique en tournant le dos aux méthodes illégales comme les attaques par saturation. Ensuite, personne ne comprend pourquoi cet Anon a retenu cette date en particulier. Elle leur semble tout à fait arbitraire, ce qui est (essentiellement) le cas, hormis le fait que le 19 septembre est la Journée internationale du parler pirate. golum se heurte donc à une vive opposition, du moins de la part de ceux qui sont devant leur écran (tous les pseudos ont été modifiés):

> <matty> pourquoi si vite?
> <golum> Parce que c'est un dimanche et que tout le monde aime les dimanches
> <matty> mais encore... pourquoi si vite?
> <golum> Parce que j'ai lancé un dé
> <golum> Et qu'il est tombé sur 19
> <golum> Je prédis que le 19 septembre les gens auront une prise de conscience
> <golum> Fais-moi confiance. Le 19 septembre.
> <fatalbert> fais-moi confiance à propos d'une date choisie sur un coup de dé

Même si tous les participants à la discussion rejettent violemment sa proposition, golum reste inflexible:

> <golum> Peu importe. Écoutez, j'ai entendu tous vos arguments contre une attaque par saturation. Mais le fait est que nous devons les réveiller.
> [...]
> <golum> Je sais bien qu'une attaque par saturation pourrait nuire à notre cause.
> <golum> Mais je crois que le jeu en vaut la chandelle.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<fatalbert> en ce qui me concerne, n'étant pas d'accord, je ne participerai pas à une attaque par saturation
<golum> Nous devons attirer l'attention
<+void> OMG C'EST ANONYMOUS, TOUT CE QU'ILS FONT C'EST DES ATTAQUES PAR SATURATION, OMGOMGOMGOMGOMG [...]
<golum> Non.
<golum> matty, comment ça s'est passé ta prise de contact avec les politiciens?
<BamBam> Ouais, j'ai toujours haï les attaques par saturation
<golum> Écoutez. J'ai saisi tous les arguments, je voulais juste dire qu'on devrait le faire.
<golum> Nous ne sommes PAS en train de mener une attaque par saturation. C'est seulement dans 20 jours.
<golum> 20 jours, c'est long

Quelques Anons énumèrent alors les risques juridiques d'une telle opération en soulignant le fait que le gouvernement des États-Unis n'est pas une cible comme les autres, puis jugent la discussion terminée. (Notons que leur évaluation des risques d'arrestation s'avérera juste: au moins 27 individus seront mis en accusation pour la série d'attaques par saturation qui suivra; d'autant qu'aux États-Unis s'en prendre à quiconque un tant soit peu célèbre peut attirer de graves ennuis.)

<matty> c'est pas justin beiber, c'est le gouv américain bordel [...]
<golum> SVP, tous, écoutez-moi quand je parle
<AnonLaw> Je vais bien me marrer quand tu iras en prison
<matty> je suis pas là pour le foutu lulz
<golum> C'est officiel. Commencez à vous préparer.

Si vous vous demandez quel sens a l'adjectif «officiel» dans le vocable d'Anonymous: oui, un projet *peut* être considéré comme «officiel» si quelqu'un l'a déclaré tel et, élément *décisif*, si assez de monde y est favorable. En cet été 2010, toutefois, les tactiques militantes d'action

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

directe ne sont pas très en vogue sur ce canal IRC. Et bien qu'un Anon ait lancé un canal IRC appelé #ddos dans le but de débattre de la possibilité d'utiliser cette tactique, les échanges d'Anonymous sur IRC ne sont libérés de toutes contraintes que jusqu'à ce qu'ils se butent à des normes et à des règles:

> <Lola> Qu'est-il arrivé à #DDoS?
> <Fred> Publie ta question ds hors-sujet stp
> <Fred> Ce canal est strictement réservé à la planification de la lutte contre l'ACTA
> <Fred> Pas au papotage
> <Lola> #ddos était un canal de lutte contre l'ACTA
> <Lola> Je veux savoir ce qui lui est arrivé
> <Fred> Les questions sur #ddos sont hors sujet
> <Fred> Ici, on parle de planification
> <Yagermister> #DDoS, c'est de la MERDE

Le lendemain, Lola revient, cette fois pour aborder la question des réseaux de machines zombies (réseaux d'ordinateurs contrôlés à distance dont on peut se servir pour intensifier une attaque par saturation):

> <Lola> avez-vous un réseau de zombies?
> <Lola> sans ça on peut pas faire grand-chose
> <Lola> on peut en obtenir à peu près 100 pour 10 $ en ce moment
> <Lola> sur les forums de skiddies*

Une fois de plus, on presse Lola d'arrêter de «discuter d'activités illégales».

*
* *

Il serait peut-être opportun que l'on se penche un peu en détail sur les réseaux de machines zombies, dans la mesure où ils occuperont une place de plus en plus importante dans les attaques par saturation attribuables à

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Anonymous, dont nous traiterons plus loin. Le phénomène présente certaines ressemblances avec le vol de bétail à l'époque de la conquête de l'Ouest. Un réseau de machines zombies consiste pour l'essentiel en un ensemble d'ordinateurs connectés à internet dont la fonction est de conférer à l'un d'eux une plus grande puissance de traitement ou des connexions réseau supplémentaires. Cette configuration permet l'exécution de tâches diverses, parmi lesquelles les attaques par saturation et l'envoi massif de pourriels. Il s'agit d'un outil très puissant, capable de répartir des tâches à des ordinateurs situés un peu partout dans le monde. Les appareils intégrés à un tel réseau le sont généralement à l'insu de leur propriétaire. Ne vous êtes-vous pas déjà demandé pourquoi votre ordinateur devenait très lent ou fonctionnait de façon bizarre? C'est peut-être parce que vous participiez sans le savoir à une attaque par saturation.

Dans la plupart des cas, un ordinateur est intégré à un réseau de machines zombies par le truchement d'un logiciel malveillant. L'infection qui peut se produire de diverses façons: par la vidéo rigolote que vous avez téléchargée, par le lien douteux que contenait un message de votre tante, par l'hameçonnage dont vous venez de faire l'objet sans vous en rendre compte ou par le virus que renfermait un logiciel téléchargé depuis internet. Une fois infecté, votre ordinateur exécute un petit programme qui d'ordinaire n'apparaît pas dans la table de processus et sert d'intermédiaire à sa participation au réseau de zombies.

Les réseaux de zombies peuvent fonctionner selon divers modes, dont un des plus communs implique le branchement des ordinateurs à un serveur et à un canal IRC spécialement configurés. Une fois la connexion établie, la machine attend patiemment les ordres du gardien de troupeau, à l'insu de son propriétaire. Le rôle du gardien est assuré par quelqu'un en mesure de diriger les composantes du réseau, soit, en général, celui ou celle qui les a infectées. La plupart du temps, cette personne attend, tapie dans le canal IRC désigné – appelé canal de commande et contrôle (C&C) –, son contentement grandissant à mesure que les machines infectées rejoignent ses rangs, tels des zombies prêts à obéir aux ordres. Le scénario typique met en scène un gardien de troupeau qui fait des allées et venues entre des

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

canaux IRC ordinaires et le canal C&C caché, qui gagne en puissance à chaque instant.

Un réseau de zombies moyen compte environ 20 000 ordinateurs, mais certains en ont recruté plus de 30 millions. (Bien que la plupart des réseaux de zombies aient mauvaise réputation – non sans raison! –, certains d'entre eux sont constitués sur une base volontaire et participative. Le plus célèbre d'entre eux est sans conteste SETI@home, qui regroupe trois millions d'appareils contribuant à la recherche d'une vie extraterrestre intelligente.) Les ordinateurs restent ainsi branchés au canal C&C jusqu'à ce que le gardien leur donne l'ordre d'accomplir une tâche. Par exemple, ce dernier n'a qu'à dire «ddos 172.16.44.1» pour que tous les zombies lancent une attaque par saturation contre cette adresse IP[10].

Les réseaux de zombies servent aussi couramment à l'envoi massif de courriels non sollicités. Car, ces pourriels étant souvent interceptés par des algorithmes qui reconnaissent leur caractère indésirable, l'adresse IP d'où ils proviennent est facilement identifiée et filtrée. Par contre, s'ils sont envoyés par des dizaines de milliers d'ordinateurs ayant chacun leur propre adresse, ils deviennent beaucoup plus difficiles à détecter et à bloquer. De ce fait, les réseaux de zombies sont souvent créés par leurs «gardiens» dans le but d'offrir leurs services à des polluposteurs.

Le contrôle de dizaines de milliers d'ordinateurs à partir d'un seul procure à la personne qui l'exerce un incomparable sentiment de puissance. En tapant de simples lignes de code, elle commande toutes ces machines; plus il y en a, plus grande est la portée des ordres qu'elle donne. L'univers des réseaux de zombies est d'ailleurs le théâtre d'une lutte incessante dont l'enjeu consiste à déterminer qui dispose du plus grand nombre de zombies, de la plus large bande passante et des machines les mieux infectées (les ordinateurs des universités, des grandes entreprises et des États disposent généralement d'une bande passante plus large).

La concurrence est si vive qu'il est courant de voir des gardiens de troupeau tenter de prendre le contrôle d'autres réseaux de zombies. Comme eux, mais obéissant à de tout autres motivations, les autorités policières et les organisations qui souhaitent en finir avec le pollupostage cherchent aussi

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

à prendre le contrôle sur ces réseaux en vue de les neutraliser. La tâche est loin d'être simple. On doit d'abord déceler le canal C&C d'où les zombies reçoivent leurs commandes. Si l'on y parvient, on peut se joindre au réseau en faisant passer son ordinateur pour une machine infectée, puis attendre un ordre. Si le gardien authentifie sa commande à l'aide d'un mot de passe, on obtient ainsi la possibilité de donner soi-même des ordres à l'ensemble du réseau[11].

*
* *

Néanmoins, comme l'indique Lola, on peut avoir accès à tout ce plaisir et à toute cette puissance moyennant un «abonnement» à prix modique. Rien à faire: les participants au canal IRC où elle intervient ne veulent pas s'abaisser à discuter réseaux de zombies et attaques par saturation. Les administrateurs du canal décident même de chasser ceux qui désirent ces attaques. Or, loin de se laisser dissuader, ces derniers deviennent des Anons nomades.

Il est sans doute ironique que golum soit devenu «une figure de premier plan de l'IFM, voire *la* figure principale du mouvement», m'explique un participant. golum est certes à l'origine du projet, mais il a vu son influence diminuer en prônant le recours à des tactiques rejetées sans appel par la majorité des membres de l'opération Chanology. En donnant «une nouvelle orientation» à l'opération, ces Anons ont veillé à ce qu'elle respecte entièrement la légalité et ont progressivement marginalisé ceux d'entre eux qui étaient restés attachés à l'action directe. Cela dit, même si l'idée de choisir une date au hasard en lançant un dé ne relève à leurs yeux que du... hasard, golum est en fait un organisateur redoutable doté d'un sens aigu de la dynamique des médias. Ayant eu l'occasion de le voir en action à plusieurs reprises, j'ai pu constater qu'il est un des meilleurs propagandistes et organisateurs d'Anonymous. En fait, devant le refus de ses pairs, golum décidera d'abandonner l'IFM pour fonder, avec quelques Anons, une nouvelle section axée sur l'action directe. Un membre de cette nouvelle

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

cellule activiste bientôt connue sous le nom d'AnonOps dira de golum qu'il «a un très bon sens de la com et de la propagande et [qu'il] a pris conscience [à ce moment-là] de l'impact psychologique considérable que peut avoir le fait d'annoncer l'anéantissement d'un site web puis de passer à l'action».

golum amène alors ses stratégies – et ses partisans – à un autre niveau. Étrangement (vu son annonce de cette date choisie sur un coup de dé), il crée un site web anti-ACTA qui propose un tout autre échéancier: un crescendo d'activités pour le 5 novembre, une date qui correspond à une journée mondiale de protestation connue sous le nom de Nuit de Guy Fawkes. golum a réparti ses activistes sur différents salons de discussion (#bump, #newor, #op) et les responsabilités.

Par contre, la confusion règne autour du moment où sera lancée la campagne d'attaques par saturation. Finalement, à l'initiative d'acteurs inconnus, elle est déclenchée à la mi-septembre, comme prévu par golum. Une vague spectaculaire d'attaques par saturation attire alors plus de 700 personnes dans le salon de discussion du groupe dissident. Elle se poursuivra pendant plus de deux mois. Tout bien considéré, les Anons ont décidé de ne pas s'en prendre au bureau du représentant au commerce. Dans le but de promouvoir le principe du partage de fichiers, ils ont plutôt choisi de se ruer sur les sites d'associations vouées à la défense du droit d'auteur, telles la Motion Picture Association of America (MPAA) et la Recording Industry Association of America (RIAA). L'événement est largement couvert par les médias, ce à quoi les membres de la nouvelle équipe prennent goût. Montrant le logo de The Pirate Bay, qui représente un galion (aussi adopté par les Anons comme symbole de la campagne), la BBC résume l'action ainsi: «Des activistes favorables au piratage se sont organisés pour attaquer des sites web de l'industrie de la musique et du cinéma[12].» Anonymous énumère tous les articles traitant de l'opération Payback (vengeance) (ainsi nommée par ses membres) sur le site tieve.tk, qui devient aussi l'endroit où s'informer alors que le collectif migre sans cesse d'un serveur IRC à l'autre, jusqu'à ce que le sien propre ne soit mis sur pied à la fin octobre.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

À partir de l'expérience que j'ai d'Anonymous, je puis affirmer aujourd'hui avec certitude que, si le groupe dissident de golum s'était contenté de rallier ses troupes avec un slogan de type «À bas l'ACTA», l'élan de soutien sans précédent dont il a bénéficié n'aurait jamais vu le jour. Mais l'esprit de Puck allait amener une délicieuse touche d'imprévu dans la vie de cette équipe en devenir. Et tout se passerait comme si Eshu, l'esprit des carrefours, avait pressé la troupe de prendre une décision. Or, comme nous le verrons, la décision prise permettra à la petite pousse de grandir et de s'épanouir pour devenir un des phénomènes politiques les plus sensationnels d'internet.

«Parfois, on doit faire un pas de plus et attaquer le site»

La nouvelle qui va changer la donne est mentionnée pour la première fois le 5 septembre 2010 dans un article d'actualité technologique publié par un média indien. Une semaine s'écoule avant que des journalistes occidentaux ne la reprennent, sa circulation se limitant d'abord à la presse spécialisée. L'article cite le directeur général d'Aiplex, une société informatique indienne qui mènerait, pour le compte d'entreprises, des attaques par saturation contre des sites de partage de fichiers tels que The Pirate Bay: «Le problème vient de sites d'échange de torrents, en général peu collaboratifs [lorsqu'on les met en demeure de retirer un film]. Dans ces cas-là, nous inondons le site d'innombrables requêtes, ce qui provoque des erreurs de base de données entraînant à leur tour un déni de service, chaque site ayant une bande passante déterminée. Parfois, on doit faire un pas de plus et attaquer le site pour en détruire les données, ce qui empêche le film de circuler davantage[13].»

Chose ironique vu la cible en cause, cet aveu prouve l'existence d'une pratique contemporaine qu'on peut comparer à celle des corsaires d'autrefois. En effet, jusqu'à ce que cela leur soit interdit en 1856, les puissances européennes employaient des pirates – les corsaires – pour certaines missions. Cette sous-traitance à des individus sillonnant les mers

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

pour leur propre compte permettait entre autres aux gouvernements de dissimuler leur implication dans des affaires douteuses. En 2010, ce n'est pas la première fois que des indices donnent à penser que les industries détentrices de droits d'auteur sous-traitent leur sale (et illégal) boulot à des spécialistes. En 2005, la MPAA a par exemple embauché un hacker qu'elle a chargé d'entrer par effraction dans les serveurs de TorrentSpy, un moteur de recherche de fichiers à partager, dans le but d'y trouver des renseignements confidentiels qui, espérait-elle, lui fourniraient des preuves de violations de la loi. Interviewé en exclusivité par *Wired*, le hacker a expliqué que la MPAA avait tenté de l'appâter avec de l'argent et des biens de luxe: «Nous avons besoin de quelqu'un comme vous. Nous vous offrons un bon poste, rémunérateur, une maison, une voiture, tout ce dont vous avez besoin [...]. Si vous acceptez de sauver Hollywood pour nous, vous deviendrez un homme riche et puissant[14].»

Mais dans le cas d'Aiplex, c'est la première fois qu'un acteur du milieu avoue aussi ouvertement se prêter à cette pratique.

Sans surprise, Anonymous et d'autres bastions geeks d'internet réagissent alors au quart de tour – et avec virulence. Car depuis plus d'une décennie, les industries détentrices de droits d'auteur, leurs associations et leurs lobbys ont investi des millions de dollars pour traquer et poursuivre sans merci les hackers responsables de sites voués au partage de fichiers comme The Pirate Bay, qui coordonnent l'accès à d'innombrables fichiers protégés par droit d'auteur. Cette fois, une partie de cette industrie a décidé de «faire un pas de plus» en confiant elle-même à des hackers le mandat d'élaborer des méthodes illégales de leur cru pour contrer le partage illicite de fichiers.

Les geeks ne manquent pas de critiquer les technologies utilisées par Aiplex (ils ont l'habitude de sauter sur toute occasion de débattre de la valeur d'une technologie). Ils se moquent de la stratégie retenue: à leurs yeux, il est aussi stupide qu'odieux de confesser un crime dans un objectif de relations publiques. Sur le populaire site d'information consacré au partage de fichiers *TorrentFreak*, un lecteur fait ce commentaire: «Aiplex cherche tout simplement, que dis-je, *quémande* les ennuis[15].»

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Ce lecteur a vu juste. La revanche prendra la forme – qui s'en étonnera? – d'attaques par saturation. Quelqu'un entreprend aussitôt de bloquer le site d'Aiplex, fort probablement à l'aide d'un réseau de zombies. golum et les autres Anons qui ont envisagé de protester contre l'ACTA en menant une campagne d'attaques par saturation profitent alors de l'occasion pour réorienter leur attention et leurs énergies vers cette affaire. Si golum et ses disciples n'ont pas hésité une seconde à laisser l'ACTA de côté pour changer de cible et établir une nouvelle date de lancement, c'est sans doute un peu parce que le hasard a joué en leur faveur, comme lors du premier coup de dé.

Sur un des premiers flyers de propagande pour l'opération Payback, la nouvelle cellule d'Anonymous admet que la campagne d'attaques par saturation a eu lieu «plus tôt que prévu» grâce à une frappe inattendue menée par un seul individu. Ses activistes y annoncent ceci: «Ce sera un bain de sang calme et bien coordonné. Nous serons sans pitié.» Avant de signer carrément: «BONNE CHASSE.»

La «chasse» d'Anonymous prendra-t-elle la forme de l'incision stratégique froide, bien huilée et sans pitié qu'annonce le flyer? Un peu. Car les premières semaines de la campagne se révèlent assez chaotiques, entre autres à cause du nombre considérable de participants qu'elle attire (du moins selon les normes de l'époque). Avec autant de monde, il est difficile de procéder de façon «calme et bien coordonnée». Lancée le 17 septembre 2010, la première attaque vise le site web de la MPAA, qu'elle bloque pendant dix-huit heures[16]. Parmi les cibles qu'Anonymous frappera pendant les quatre jours suivants, mentionnons la fédération internationale de l'industrie phonographique (OFPI), Aiplex (naturellement!), la RIAA et ACS:Law, un cabinet d'avocats britannique qui défend les intérêts des industries détentrices de droits d'auteur. Du point de vue de ces Anons rebelles, l'opération Payback est un succès retentissant, et la presse n'a d'autre choix que de publier de nombreux articles à son sujet.

Un des exploits les plus remarquables de l'opération Payback est la façon dont AnonOps parvient, à l'aide de son seul matériel de propagande, à faire croire aux médias (et à une bonne partie de ses propres membres!)

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

que la MPAA a retenu les services d'Aiplex. Cette hypothèse ne repose sur aucune preuve. De nombreux observateurs affirmeront quelques années plus tard que la firme a plutôt été embauchée par Bollywood. Le 27 septembre 2010, pourtant, des dizaines de médias réputés, dont Reuters, publient des affirmations comme celle-ci, sans disposer de preuves dignes de ce nom: «mpaa.org et le site web d'Aiplex Software, une entreprise embauchée par la MPAA pour lutter contre les sites qui se livrent à la piraterie, ont été mis hors service pendant une bonne partie de la journée, selon le blog sur le piratage *TorrentFreak*[17]». À force de lire et de relire ce bobard dans les médias, j'en viendrai moi-même à le répéter en maintes occasions. Encore aujourd'hui, j'ignore qui l'a rapporté pour la première fois et s'il est le fruit d'un quiproquo authentique (les activistes de la base étant très nombreux à y avoir cru) ou d'une mystification intentionnelle. Quoi qu'il en soit, Anonymous développera cette spécialité nouvellement découverte qui consiste à tromper les médias.

Après quelques jours de campagne, c'est l'attaque la plus réussie de la saison d'AnonOps qui est sur le point de débuter. La cellule s'y révélera sans merci. L'organisation visée, ACS:Law, sera couverte de honte avant de sombrer dans l'oubli grâce à une première fuite d'envergure révélée par Anonymous. Voici les détails.

«Les dix minutes de retard de mon train [...] me préoccupent beaucoup plus que le temps qu'ils me font perdre avec leurs conneries»

Pour l'équipe hétéroclite rassemblée dans le cadre de l'opération Payback, la MPAA était donc au début une cible de choix. Toutefois, le 21 septembre, Anonymous doit se rendre à l'évidence: ils ne semblent plus arriver à bloquer le site de cette association, car elle a confié à une firme externe le mandat de la protéger contre les attaques par saturation. Ce jour-là, à la suite de vigoureux débats, les Anons décident donc de se tourner vers le

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

cabinet d'avocats ACS:Law, tristement célèbre pour ses lettres de menaces envoyées pour le compte d'ayants droit à des milliers de personnes soupçonnées d'avoir partagé des fichiers, à qui il a réclamé un dédommagement et la cessation de tout téléchargement apparemment illégal. Anonymous mettra plus de temps à choisir ACS:Law (deux heures) qu'à en bloquer le site web (deux minutes). L'avocat principal du cabinet, Andrew Crossley, n'est guère impressionné par l'attaque, à laquelle il réplique spontanément par cette déclaration: «Le site n'a été bloqué que pendant quelques heures. Les dix minutes de retard de mon train ou la file d'attente que je dois me taper pour avoir mon café me préoccupent beaucoup plus que le temps qu'ils me font perdre avec leurs conneries[18].»

Mais ces quelques heures d'interruption lui auront probablement coûté la mort de son cabinet, comme en témoigne la suite des événements. L'équipe web d'ACS:Law fait montre d'une telle incompétence en restaurant le site qu'elle en effectue une sauvegarde complète, avec tous les courriels et mots de passe, qui deviennent ainsi accessibles à quiconque possède un minimum de compétences techniques. Des Anons s'en rendent compte et s'emparent de tous les courriels, qu'ils s'empressent de télécharger sur The Pirate Bay. Anonymous vient ainsi d'inaugurer une série de fuites proprement hallucinantes qui viendront prouver l'existence de manquements graves de la part du cabinet.

Précisons que le cabinet de Crossley est alors déjà dans la mire du gouvernement. Quelques mois auparavant, le journaliste spécialisé en technologie Nate Anderson a en effet rapporté ce qu'il a qualifié de «débat houleux» entre les membres de la Chambre des lords. En procédant à l'examen d'un amendement intitulé «Recours contre les menaces non fondées de poursuites judiciaires pour violation du droit d'auteur», de nombreux lords ont critiqué les méthodes d'ACS:Law[19]. Lord Lucas, qui avait proposé l'amendement, a eu des mots particulièrement durs à l'endroit du cabinet d'avocats: «Nous devons faire quelque chose à propos du montant des dommages-intérêts réclamés. Dans la cadre d'une procédure civile sur une question technique, on parle carrément de chantage; on

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

estime qu'il en coûte 10 000 livres sterling pour se défendre dans de tels cas[20].»

Les courriels obtenus par Anonymous contribuent tout simplement à confirmer, avec des détails beaucoup plus précis et incriminants, les attaques incessantes d'ACS:Law contre de prétendus contrevenants au droit d'auteur[21]. Une des tactiques du cabinet consiste à envoyer à des hommes mariés des lettres affirmant qu'ils ont téléchargé de la pornographie homosexuelle; ils sont nombreux à avoir payé de 500 à 600 livres sterling à ACS:Law pour qu'on les laisse tranquilles[22]. Cette fuite de courriels portera un coup fatal au cabinet d'avocats, qui fermera ses portes en février 2011[23].

Notons une fois de plus que la décision d'AnonOps d'attaquer ACS:Law a été prise, comme bien d'autres, dans le feu de l'action. Si le groupe avait voté autrement, l'opération n'aurait jamais eu lieu. Il vaut la peine de se pencher un moment sur son mécanisme décisionnel, dont la campagne contre le cabinet d'avocats offre un excellent exemple.

À son apogée, le canal IRC public #savetpb (pour «Save The Pirate Bay», qui deviendra plus tard #operationpayback) compte plus de 1 000 participants. Nombre d'entre eux proviennent de 4chan, où les nouvelles de l'affaire Aiplex se sont répandues comme une traînée de poudre et ont incité beaucoup de monde à passer à l'action. On encourage les participants aux canaux publics à utiliser un outil appelé «Low Orbit Ion Cannon» (LOIC, canon à ions en orbite basse), dont le slogan est «Quand les harpons, les frappes aériennes et les bombes atomiques ne suffisent plus à la tâche». LOIC est un logiciel libre qui permet à ses utilisateurs de contribuer à une attaque par saturation depuis le confort de leur foyer: il leur suffit de taper une adresse IP (annoncée sur un canal IRC) et d'appuyer sur un gros bouton sur lequel est écrit «IMMA CHARGIN MAH LAZER» (qu'on pourrait traduire par «Je charge mon laser»). Ce faisant, un internaute peut se joindre au chœur des protestataires qui envoient des requêtes à un serveur; il peut aussi configurer LOIC en «mode ruche*», qui permet à son appareil de contribuer automatiquement au *botnet** volontaire.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Au même moment, sur un canal IRC privé d'abord appelé #savetpbmods, mais qui sera vite rebaptisé #command, d'autres Anons mènent un débat intense, souvent houleux et pour le moins confus, sur la stratégie à adopter et les cibles à viser. La plupart des participants au canal public ignorent l'existence de ce canal privé, à moins d'y avoir été admis par cooptation. Dans une interview, un des fondateurs de #command en révélera les critères d'admissibilité: «Un membre peut vous inviter si vous vous êtes montré productif, utile ou digne de confiance.»

Sont reproduits ci-dessous d'infimes extraits de la conversation on ne peut plus alambiquée (mais non dépourvue de cohérence) qui, en quelque deux heures, conduira à la décision d'attaquer ACS:Law. Le processus s'avère assez fluide et informel. Les premières personnes à intervenir constatent le nombre impressionnant d'individus rassemblés sur le canal public, lesquels attendent en quelque sorte les ordres:

<Anon2> 660 personnes et +
<Anon5> eh bien
<Anon5> ça chie
<Anon6> ouais [...]
<Anon4> ça a magistralement chié
<Anon7> le dispositif [de la MPAA] contre les attaques par saturation marche
<Anon7> je propose de changer de cible
<Anon7> bpi [British Phonographic Industry]?
<Anon8> pourquoi pas la riaa?
<Anon7> parce qu'on a raté bpi la dernière fois, on n'était pas assez nombreux

Au fil de la conversation, l'affluence continue d'augmenter sur le canal public. Les participants commencent à se préoccuper du dynamisme et du moral des troupes:

<Anon1> pendant ce temps, il y a plein d'articles qui disent qu'on a quand même fait beaucoup de dégats

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<Anon8> qu'a fait bpi?
<Anon7> ma foi...
<Anon9> les gars, pas de mélodrame dans le fil de discussion principal
<Anon9> on est là pour s'occuper du moral des troupes [...]
<Anon9> or même si on ne fait qu'ÉVOQUER que nos efforts sont «vains», les gens vont partir en masse
<Anon9> le moral des troupes a toujours été déterminant
<Anon9> les 800 personnes ne sont pas là parce qu'on dit la vérité
<Anon9> elles sont là parce qu'elles CROIENT qu'elles sont en train de faire quelque chose
<Anon7> Les gars, je ne veux PAS échouer aux yeux du public ni que nos troupes nous lâchent. Nous devons trouver une autre cible au plus vite.

Le désaccord à propos de la cible prend de l'ampleur. Quelqu'un fait remarquer que la campagne n'a pas vraiment nui aux finances de la MPAA, comme en fait foi la forte somme que l'association a investie dans la protection contre les attaques par saturation. D'un commun accord, les participants décident donc de cesser de s'en prendre à la MPAA et de choisir une autre cible. Quelqu'un affirme qu'il faut considérer la campagne «comme une expérimentation, quel qu'en soit l'objectif. Prouvez-moi que j'ai tort». Alors que les participants croient avoir atteint un consensus, l'un d'eux se récrie et demande le vote; comme c'est souvent le cas lors de réunions par IRC (et au superlatif dans le cas d'Anonymous), la conversation devient alors encore plus confuse:

<Anon7> Nooon
<Anon7> Attendez
<Anon7> Votons
<Anon8> On a l'opinion publique de notre côté parce qu'on n'attaque pas des sites au hasard
<Anon7> Commençons par désigner des sites

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<Anon7> Jusqu'ici, la riaa et bpi ont été nommées
<Anon7> Il y en a d'autres?
<Anon9> Je pense que qu'on a trouvé l'idée parfaite
<Anon7> Nous pouvons voter ici
<Anon16> Salut
<Anon1> laissons Anon9 s'exprimer
<Anon9> Je pense que je suis d'accord avec Anon13: ACS:Law
<Anon9> Allons-y à fond
<Anon9> On s'attaque à leur site merdique, on balance des articles qui parlent d'eux, etc.
<Anon9> Si on change de cap maintenant, on n'aura PAS le temps de se préparer
<Anon1> ok, on met un nouveau flyer sur /b/ avec la cible de demain, à la même heure?
<Anon10> Va pour ACS:Law pour moi aussi
<Anon4> moi aussi
<Anon13> Est-ce qu'on devrait changer le sujet de la conversation principale et demander aux lazers de prendre la nouvelle cible tout de suite, histoire de ne pas perdre trop de monde? ou attaquer demain, au risque d'en avoir perdu des centaines?
<Anon8> donnez-moi une aussi bonne raison de choisir une cible [...]
<Anon7> on vote?
<Anon13> Je vote pour ACS
<Anon7> Attaque par saturation contre ACS:Law. 1 = oui, 2 = non

Pendant que certains participants passent au vote, d'autres poursuivent le débat sur le choix de la cible. «Attaquer des organisations antipiratage choisies au hasard n'aide pas notre cause», soutiennent-ils. Ils suscitent ainsi la tenue d'un autre tour de scrutin, qui s'avère long et fastidieux. Au

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

bout de deux heures, ils semblent enfin proches d'un accord. Mais devinez ce qui se passe?

> <Anon7> www.acs-law.org.uk
> <Anon12> Donne-moi l'info que j'ai demandée
> <Anon7> www.acs-law.org.uk est bloqué. DÉJÀ! [...]
> <Anon12> quoi???
> <Anon12>?
> <Anon1> OMG?
> <Anon13> Ça a été rapide.
> <Anon1> combien de temps avons-nous mis à voter une deuxième fois? XD
> <Anon14> plus que le temps que ça a pris pour fermer le site

Un participant s'est sans doute dit que le consensus était assez large pour aller de l'avant et a lancé les *botnets*.

Deux heures de planification. Deux minutes d'attaque par saturation. Un cabinet d'avocat qui ferme ses portes peu de temps après. Un peu plus d'un an après la fuite de courriels orchestrée par Anonymous, Crossley, l'homme qui n'aime surtout pas faire la queue pour un café, sera traduit devant le tribunal disciplinaire du barreau sous plusieurs accusations. Il plaidera coupable pour six d'entre elles, dont celles d'«avoir agi de manière à ébranler la confiance du public en lui ou en la profession d'avocat» et de «s'être servi de son statut d'avocat pour tirer un avantage personnel indu des destinataires des lettres[24]». Il sera condamné à 76 000 livres sterling d'amende et verra sa licence suspendue pour deux ans. On lui reprochera également de ne pas avoir pris les mesures nécessaires pour protéger les données de sa clientèle, ce qu'il contestera en vain: il sera déclaré coupable, et le bureau du commissaire à l'information le mettra à l'amende pour atteinte à la sécurité des données[25].

Même si une bonne partie des actions d'Anonymous ne visent qu'à attirer l'attention des médias pour faire connaître un enjeu, le sort leur réserve parfois d'heureuses surprises. Comme une occasion d'enrayer la corruption.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Les armes des geeks (qui sont rarement d'accord entre eux)

En multipliant les actions directes au cours de l'automne 2010, AnonOps a donné un nouveau souffle à l'idée encore neuve selon laquelle Anonymous pourrait être synonyme d'activisme. Jadis exclusivement associé aux formes les plus abjectes de trollage, le nom en est progressivement venu à désigner une branche irrévérencieuse de la dissidence. Notons toutefois que golum, les Anons cités ci-dessus et les autres responsables des campagnes de septembre et d'octobre n'avaient pas en tête de constituer une équipe – et encore moins un réseau – qui durerait plus de quelques semaines. Cependant, comme si les événements ayant fait de l'opération Chanology une entité distincte s'étaient répétés, la reconnaissance des médias a contribué à la solidification de cette nouvelle cellule. Un collaborateur de *TorrentFreak* a rapporté les circonstances de cette évolution: «Les membres de #command ont été "agréablement" surpris par l'importante couverture médiatique dont l'opération a fait l'objet, mais se sont demandé quelle direction ils allaient prendre à partir de là. Propulsés au centre de l'attention, ils n'avaient pas de plan. Ils ont fini par continuer dans la même voie, celle des attaques par saturation. [...] L'attention des médias fait effectivement partie des facteurs ayant amené l'opération à se poursuivre[26].»

L'inscription d'AnonOps dans la durée a fait apparaître les clivages opposant les diverses cellules militantes d'Anonymous. Les deux groupes les plus actifs du collectif, Chanology et AnonOps, n'auraient pu être plus différents l'un de l'autre en termes de tactique: le premier respectait généralement la loi, tandis que le second la transgressait avec avidité et enthousiasme. D'ailleurs, dans un geste de reconnaissance de ces querelles intestines et de ces élans sectaires, Anonymous adoptera plus tard le leitmotiv «Anonymous n'est pas unanime» (*Anonymous is not unanimous*[27]).

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

C’est à peu près à cette époque que j’ai commencé à saisir la signification globale de l’apparition de ces geeks et hackers disparates – Anonymous (AnonOps contre Chanology), Assange, Manning, The Pirate Bay et les autres – qui, plus nombreux que jamais, avaient fait leur entrée dans l’arène politique. En orchestrant leur contestation autour d’un ensemble d’enjeux (en particulier les libertés civiles), ils ont transformé la vie politique, le droit, les représentations médiatiques et l’opinion publique. Quoique se démarquant par sa grandiloquence et son inconstance, Anonymous a indéniablement contribué à créer un vivier de hackers et de geeks décidés à prendre à bras le corps les enjeux politiques et à se faire entendre.

Anonymous révèle l’importance croissante de ce que j’appelle les «armes des geeks» (*weapons of the geek*, par contraste avec *weapons of the weak*, qui signifie «armes des faibles», terme employé par l’anthropologue James C. Scott dans un ouvrage portant ce titre où il décrit la nature clandestine de la résistance politique de paysans malaisiens). Là où la notion d’«armes des faibles» désigne les tactiques mises en œuvre par des populations économiquement marginalisées sous forme d’actions illégales à petite échelle et apolitiques en apparence (comme le vandalisme ou le retard volontaire), les «armes des geeks» représentent un mode d’action politique exercé par une classe d’acteurs sociaux privilégiés et en vue, qui sont souvent au cœur de la vie économique.

Le hacking politique n’est pas déterminé de façon grossière par la technologie, même si dans les faits, les expériences technologiques donnent forme à son expression. Comme il existe diverses manières de faire du hacking, il existe diverses manières pour les hackers de prendre part au débat politique. De l’élaboration de politiques aux actes risqués de désobéissance civile, en passant par l’engagement dans un Parti pirate et la redéfinition du droit par le biais des logiciels libres, les geeks et hackers ne sont pas liés à une idéologie unique (le libertarianisme, par exemple) et sont loin d’être unanimes quant à la voie que devrait emprunter le changement social.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Ils partagent cependant le fait que leurs outils – et, dans une moindre mesure, leur sensibilité – politiques naissent de l'expérience concrète de leur savoir-faire, qu'il s'agisse de l'administration d'un serveur ou de montage vidéo. Ils mettent souvent leurs compétences au service du renforcement des libertés civiles, comme le droit à la vie privée. Contrairement aux paysans, qui souhaitent passer inaperçus, les geeks et les hackers (y compris les anonymes d'Anonymous) cherchent ouvertement à attirer l'attention par le caractère éphémère et souvent controversé de leurs actions. À l'automne 2010, AnonOps était ainsi à l'avant-garde d'expériences qui visaient à tester les nouvelles possibilités de désobéissance civile numérique et leurs limites juridiques.

Si des gens du milieu ont perçu ces expériences comme une réussite, d'autres (dont certains faisaient partie du même camp) se sont montrés franchement méfiants à l'égard des tactiques adoptées. Le Parti pirate, en particulier, n'était guère emballé par le recours à l'attaque par saturation à des fins politiques. Fondé en 2006 par le Suédois Rickard Falkvinge, militant pour une culture libre, ce parti politique a fait des avancées en Europe et en Australie mais ne dispose que d'une très faible base en Amérique du Nord. Sa plateforme actuelle propose essentiellement une réforme du droit d'auteur et l'élaboration d'outils pour une démocratie directe; elle prône notamment un internet libre et la défense des libertés civiles. Les partis pirates du Royaume-Uni et des États-Unis ont demandé par écrit à AnonOps de cesser immédiatement toute attaque par saturation[28]. (Notons que la lettre a suscité de vifs débats non seulement chez les participants d'AnonOps, mais aussi chez les membres du Parti pirate eux-mêmes.)

> L'opération Payback doit prendre fin. Bien qu'elle témoigne sans doute d'une frustration de plus en plus répandue devant des lois constamment réécrites dans le but de tuer notre culture créatrice au nom de la rentabilité, ses méthodes nuisent davantage à l'objectif visé qu'elles n'y contribuent.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> Si vous poursuivez vos attaques, vous porterez préjudice à ceux et celles qui militent pour réformer le droit d'auteur et réduire les abus, mais qui le font en respectant la loi. Car lorsqu'ils ou elles plaideront pour une réforme du droit d'auteur sur la base de sa propre valeur, on les accusera de soutenir des criminels et le non-respect des lois. Parlementaires et médias pourront alors encore plus aisément se voiler la face quant aux avantages manifestes d'un régime de droit d'auteur équitable et de la liberté d'expression, ainsi que réclamer des lois plus dures contre «ces pirates et ces hackers»[29].

Chose sans doute surprenante, des participants au canal privé #command ont brièvement souscrit à l'appel du Parti pirate et envisagé de renoncer aux tactiques illégales pour adopter des méthodes plus modérées de type réformiste, telle la formulation d'une liste de revendications. Interviewé dans l'article de *TorrentFreak* cité précédemment, un des principaux organisateurs de l'opération a notamment révélé l'existence du canal secret et affirmé que ses participants avaient opté pour des tactiques respectueuses de la loi.

> Le noyau restreint est constitué du canal IRC #command. Il joue en quelque sorte un rôle d'intermédiaire entre ses membres et l'attaque proprement dite. Un autre groupe de participants sur IRC (le canal principal #operationpayback) n'existe que pour tirer sur les cibles. [...] La semaine dernière, #command a choisi de mettre la pédale douce sur les attaques par saturation et d'opter pour une autre stratégie, essentiellement pour redevenir le centre de l'attention. Ses membres ont décidé de présenter une liste de revendications aux gouvernements du monde entier. Allant contre ses influences les plus anarchistes, #command a décidé de prendre part au débat politique[30].

Cette double nouvelle (l'existence d'un canal secret et la volonté de ses membres d'embrasser la légalité) a été très mal accueillie par les participants au canal IRC public #operationpayback. Elle a pratiquement provoqué une mutinerie. Gobo (pseudo modifié), un acteur central du canal

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

public qui se joindrait ultérieurement à un autre canal secret revigoré par la révélation, explique: «Cet article a vraiment fait chier beaucoup de monde sur le canal principal. Une bonne partie du grabuge a été liée au fait qu'Anonymous était un mouvement sans chef: "Mais pour qui ils se prennent?" D'une certaine manière, les gens de #command ne se sont pas vraiment rendu compte de la controverse qu'ils ont provoquée en outrepassant les limites de leur fonction (telles que définies par les participants au canal principal)[31].»

La plupart des Anons qui criaient leur indignation ignoraient l'existence d'un canal IRC encore plus secret que l'autre, #internetfeds. Créé à l'origine dans le but de faciliter l'exécution d'opérations (en particulier le hacking clandestin), il était resté inactif pendant un certain temps. Un de ses membres avait alors contacté Gobo et l'avait invité à s'y joindre en vue de le réactiver. L'engagement qu'avait pris AnonOps de mettre un terme aux attaques par saturation devenait ainsi pour le moins douteux: «On pourrait résumer l'idée ainsi: conformément à la lettre du Parti pirate, l'opération Payback s'engagerait publiquement à "cesser toute activité illégale". Ces activités seraient prises en charge à titre privé par #internetfeds au nom d'"Anonymous", et surtout pas au nom de l'opération Payback. L'existence du canal serait gardée secrète pour ne pas compromettre la nouvelle image de "contestation légitime" que #command souhaitait donner à l'opération Payback[32].»

Ainsi, un groupuscule issu d'une petite faction planifiait de raviver une autre faction encore plus petite et souterraine – qui, toutefois, ne respecterait qu'approximativement le principe selon lequel elle devait taire son existence (elle agissait peut-être en secret, mais chacun de ses défaçages était signé d'un logo où figurait son nom: «Anéanti par #internerfeds[33]»). En fin de compte, #internetfeds n'aurait pas besoin de mener à bien ce projet de mission «religieusement secrète», car les membres du canal principal ont dit aux types de #command d'aller se faire voir et ont réaffirmé leur intention de continuer à lancer des attaques par saturation, avec ou sans eux: la «guerre civile» avait éclaté sur le canal public où, selon Gobo, la plupart des gens «condamnaient vivement non

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

seulement l'idée de respecter la loi, mais plus précisément le fait que les membres de #command s'étaient comportés en grossiers *leaderfags* en prenant cette orientation sans même en informer le canal principal. Une altercation cinglante a suivi, puis quelqu'un a simplement invité les participants à oublier le mode ruche de LOIC et à frapper la prochaine cible manuellement, avec ou sans le soutien de #command[34]».

Touchés par la colère des masses d'IRC, les membres de #command sont «presque immédiatement revenus sur leur engagement de rendre l'opération légale», raconte Gobo. Même si, en théorie, #internetfeds n'était plus nécessaire à cette campagne en particulier (#command ayant renoué avec les attaques par saturation à la suite des pressions exercées par les membres du canal public), le canal clandestin serait maintenu et finirait par devenir ce que Gobo qualifie de «canal extrêmement militant voué au défaçage et aux fuites». Son heure de gloire viendrait quelques mois plus tard. La paix était revenue, mais tout juste.

Légitimité contre légalité

En septembre 2010, la nouvelle cellule d'Anonymous née de l'indignation qu'inspirait le double jeu des industries détentrices de droits d'auteur semblait toujours au bord du chaos. Souvent passionnées, désordonnées, spontanées, ses actions procuraient des sensations fortes à tous ceux qui y participaient. Peu à peu, les membres d'AnonOps en sont venus à prendre leurs décisions de façon plus réfléchie, conséquence directe d'une réflexion collective sur la notion même de collectivité. La question du mode d'organisation a sans aucun doute été soulevée par de nombreux participants outrés par le double standard qu'ils avaient subi lors des premières campagnes. Un des principaux hackers du groupe m'a expliqué pourquoi il estimait justifié d'aller de l'avant avec les méthodes illégales, un sentiment qui semble bien traduire l'ambiance qui régnait alors: «J'y voyais une forme de justice poétique en réaction aux attaques par saturation menées par Aiplex contre The Pirate Bay.» Gobo, qui a travaillé en étroite

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

collaboration avec golum, se souvient qu'il «s'insurgeait toujours avec passion contre le fait que des membres d'Anonymous [s'étaient fait arrêter pour avoir participé à des attaques par saturation motivées par le trollage] alors que de gros bonnets se vantaient de faire la même chose en sachant qu'ils ne seraient jamais poursuivis. Pour golum, les doubles standards n'avaient pas leur place en politique: "des entreprises commettent des crimes en toute impunité" alors que les gens ordinaires, eux, ne peuvent pas échapper à la loi[35]».

En novembre, des sentiments individuels comme celui-ci ont résulté en une déclaration politique collective. Peu après avoir tourné le dos à leur intention d'embrasser la légalité, les membres d'AnonOps ont écrit une lettre au Parti pirate. Le groupe y allait d'un éloquent plaidoyer en faveur des attaques par saturation en faisant valoir la primauté de la légitimité sur la légalité:

> Anonymous et l'opération Payback ont des valeurs et des objectifs (liberté d'information, d'expression et de partage) en commun avec les Partis pirates, mais nous sommes des organisations totalement indépendantes.
>
> Nous ne nous intéressons pas à la légalité, mais à la légitimité. Ceux qui font les lois sont ceux-là mêmes qui ont décidé que le harcèlement du public au sujet du droit d'auteur, de l'érosion des libertés civiles et des abominations censoriales comme la COICA [Combating Online Infringement and Counterfeits Act (loi américaine visant à contrer les infractions et la contrefaçon en ligne)], l'ACTA et la DEA [Digital Economy Act (loi britannique sur l'économie numérique)] sont de bonnes choses qui doivent être imposées à la population. Elles appliquent leurs propres lois de façon sélective en épargnant les organisations «officielles» qui se livrent à des pratiques comme les opérations d'extorsion à grande échelle (poursuites délibérées contre des milliers d'individus pour violation du droit d'auteur sans preuve suffisante) ou les attaques par saturation de sites

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

qui nuisent à leurs intérêts (Aiplex). En raison de leur hypocrisie pure et simple, nous ne reconnaissons pas leur «autorité».

Enfin, nous reconnaissons et respectons le travail des partis pirates, à qui nous souhaitons bonne chance. Nous espérons que vous continuerez votre lutte comme nous continuons la nôtre[36].

Comme en fait foi cette lettre, AnonOps avait entrepris une réflexion et n'hésitait plus à inscrire ses activités dans l'ordre de la désobéissance civile. Peu après que ses membres se furent entendus, en novembre, sur la question des attaques par saturation, le nombre de participants fréquentant son serveur IRC a connu une chute précipitée. Seules quelques cellules secrètes se sont maintenues, bien planquées dans leurs canaux distincts et clandestins. Il était impossible de prévoir que, trois semaines plus tard, AnonOps lancerait la plus vaste campagne de désobéissance civile d'attaque par saturation de tous les temps.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Chapitre 4

Le coup que le monde entendit

Je n'ai qu'une minute
Tout juste soixante secondes
On me l'a imposée, je ne peux la refuser
Je ne l'ai pas cherchée, je ne l'ai pas choisie
Mais il ne tient qu'à moi de l'utiliser
Je devrai souffrir si elle m'échappe,
m'expliquer si j'en abuse
Juste une toute petite minute
Mais dedans, il y a l'éternité

Benjamin Elijah MAYS, enseignant américain et président de l'université Morehouse

POUR BIEN DES COMMENTATEURS, Anonymous est une entité primordiale amorphe, encore à l'état d'ectoplasme, un non-être mythique dont l'existence ne devient concrète que si un observateur extérieur prononce son nom. Certains laissent alors entendre que, suivant cette logique, le collectif et ses interventions souffrent d'un manque de cohésion. «Le message nébuleux de ce groupe sans porte-parole, sans chef et sans un projet politique clair qui lui donnerait une orientation stable n'est pas aidé par une idéologie qui oscille entre l'extrême gauche, l'extrême droite et des positions plus modérées», écrivait Art Keller dans le magazine *Newsweek* en 2013[1]. Un Anon m'a lui-même donné un exemple plus prosaïque de cette perception lors d'une séance de chat privée: «J'ai parlé d'Anonymous avec un ami du monde réel aujourd'hui. J'ai eu l'impression qu'il y voyait des cerveaux désincarnés, suspendus en orbite pour livrer bataille à des

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

satellites, ou quelque chose du genre. Il semblait sidéré par l'idée que des personnes en chair et en os aient quelque chose à y voir.»

Non seulement ces généralisations, propagées tant par les médias que par le commun des mortels, sont fausses pour la plupart, mais elles nuisent aussi à la compréhension du phénomène Anonymous. Loin d'être dépourvu de structure ou de s'agiter dans tous les sens comme une boussole au pôle Nord, le collectif est le théâtre d'une myriade de relations, de structures et de positions morales. Des êtres humains (qui s'expriment, codent, débattent, se querellent, créent et jouent) sont présents à chaque étape d'une opération. J'ai eu droit à une expression particulièrement charmante de ce sentiment lors d'une conversation avec Mustafa Al-Bassam, ex-membre important de LulzSec, un groupe de hackers ayant rompu avec Anonymous. Un jour où je n'en pouvais plus de répertorier le moindre canal secret et de classer la moindre observation, je l'ai trouvé en ligne et me suis mise à le harceler (à le supplier, en fait) pour qu'il me fournisse une liste ordonnée et précise de tous les canaux Internet Relay Chat (IRC) auxquels il pourrait songer. Il a gentiment accepté, puis, au beau milieu d'une de ses explications méticuleuses (aujourd'hui toujours aussi opaques pour moi), il m'a demandé: «Connaissez-vous *kittencore*?»

Misère, pas la kittenporn[2]? me suis-je dit. Il a immédiatement (et heureusement) mis un frein à mon imagination: «Le canal IRC. Nous avions un canal appelé #kittencore et un autre appelé #upperdeck. Tous deux avaient les mêmes membres, sauf que #upperdeck en comptait un de moins.» Je lui ai demandé pourquoi ils laissaient l'un d'entre eux dans l'ignorance. «Parce qu'il était arrivé dans le décor très tard et que nous étions réticents à l'accueillir au centre, et aussi parce qu'il était arrivé au moment même où nous partagions les bitcoins», m'a-t-il répondu.

«De la micro-micropolitique et des factions dans d'autres factions», ai-je répliqué.

C'est précisément ce mixte de précision et d'abondance (un canal, exactement comme les autres, mais avec en moins une personne jugée néophyte et pas encore digne de confiance) qui rend Anonymous si difficile à décrire et à catégoriser. L'idéal d'auto-effacement de l'individu permet

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

aux membres du collectif de fusionner leurs esprits, en quelque sorte, et de faire ainsi vivre un mouvement en perpétuelle émergence et en constante évolution. Quantité de relations, de fiefs et de cliques y coexistent à l'insu du grand public, qui observe généralement Anonymous à travers le filtre d'une propagande savamment orchestrée et du point de vue plutôt prévisible des médias.

Et pourtant, si l'on regarde au-delà de l'ordinateur, on constate à tout moment qu'Anonymous est assimilable à un agrégat de chair et d'os (intégrés grâce à des câbles, à des transistors et à des signaux wi-fi) où abondent des kilomètres de vaisseaux chargés de sang, des kilos de viscères débordant de fluides vitaux et un enchevêtrement de transmetteurs de signaux, le tout soutenu par un squelette auquel sont attachés des pistons musculaires, et coordonné depuis un dôme caverneux renfermant un centre de contrôle toujours actif – analogue de ces systèmes fabuleusement grotesques et chaotiquement précis qui, considérés isolément, constituent ce qu'on appelle des personnes. Les membres d'Anonymous sont pareils à nous tous. Ce sont des humains ordinaires assis devant leur écran et tapant sur leur clavier comme leurs congénères ont coutume de le faire en cet instant précis de la longue trajectoire de la condition humaine. Chaque corps pris isolément est le vecteur d'un récit de vie irréductiblement singulier et complexe (dans lequel s'incarne la multiplicité des phénomènes sociaux) qui peut lui-même se résumer à la succession d'événements qui le composent: la course des doigts sur le clavier et le mouvement épisodique de la souris qui s'enregistrent ailleurs, sur un écran, sous la forme d'un texte en deux dimensions ou d'une vidéo en trois dimensions; la musique de tous ces doigts qui résonne en une symphonie bien orchestrée (quoique cacophonique et souvent discordante); une symphonie atonale et sans mesure aux thèmes vils et obscènes, mais fascinante aux oreilles de certains: l'épopée mythique d'Anonymous.

Anonymous n'a pas toujours été aussi complexe: ce n'est que vers la toute fin de 2010 que le collectif activiste s'est mué en un enchevêtrement labyrinthique en constante transformation. En novembre 2010, en effet, le Minotaure qui parcourait son dédale n'avait pas encore trouvé la sortie vers

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

le monde extérieur. Mais il s'en rapprochait. L'opération Chanology se poursuivait, et le canal IRC d'AnonOps demeurait le centre névralgique d'une série d'attaques par saturation contre les industries détentrices de droits d'auteur. Fin novembre, cette succession ininterrompue d'actions directes pour le partage de fichiers prit subitement fin; la participation aux canaux IRC publics tomba alors à son plus bas niveau. Mais le noyau dur, dont les membres collaboraient sur les canaux privés, ne décida pas de fermer boutique pour autant (bien que ce faible taux de participation les préoccupât bel et bien). Il profita plutôt de l'occasion pour mieux s'organiser: une séance de *brainstorming* déboucha sur la rédaction collective d'un document précisant les objectifs et la structure du canal privé #command, qui avait fait scandale dans les rangs des Anons lorsque son existence avait été révélée quelques semaines auparavant (voir l'encadré suivant).

Le document délimitait d'abord le rôle de #command en précisant que le canal était «un intermédiaire [qui] ne prend pas lui-même de décisions» et coordonnait «uniquement les débats, et non la direction» des opérations. Il se concluait par une liste de règles, dont une proclamait non sans ironie que «seuls les adultes» étaient autorisés à faire partie du «commandement» (#command). (L'ironie vient du fait que certains membres sont mineurs – du reste, peut-on vraiment parler d'un Anonymous... «adulte»?)

Règles de #command

- Nul ne peut chasser ou, pire encore, bannir quelqu'un de #command.
- N'interrompez pas un sujet lancé par quelqu'un d'autre.
- Commencez par dire de quoi il est question, puis établissez des priorités.
- Quiconque fait du trollage sur #command sera retiré (pour de bon) de la liste AOP.
- Les querelles personnelles sont taboues.
- Seules les grandes personnes sont admises.
- Évitez tout propos hors sujet dans les discussions (entre administrateurs).
- Identifiez les problèmes de façon structurée: cernez le problème, proposez une solution. En l'absence de solution, étayez votre argumentation – si celle-ci est valable! – par des preuves ou des arguments.
- S'il y a quelqu'un que vous n'aimez pas, revenez-en. On est tous dans le même bateau.
- Les administrateurs et les IRCops sont censés donner l'exemple; faites comme eux!
- Ne vous attendez pas à ce que les IRCops règlent tous vos problèmes. Essayez d'abord de les régler vous-mêmes, puis, si vous n'y arrivez pas, demandez l'aide d'un IRCop.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Ce document était truffé de concepts qui pourraient être jugés ésotériques par quiconque n'aurait jamais fréquenté les réseaux IRC; quelques explications s'imposent donc. Pour se brancher à un serveur IRC, on doit utiliser un logiciel client. On choisit ensuite un pseudo (certaines personnes s'inscrivent sous leur vrai nom, mais le recours au pseudo est nettement plus répandu). On peut discuter en tête-à-tête avec d'autres utilisateurs ou encore se joindre à des «canaux», désignés par un nom précédé d'un dièse (#) et accessibles à quiconque en connaît l'existence, à moins qu'il s'agisse d'un salon accessible uniquement sur invitation. Une fois branché au canal, on peut discuter avec les utilisateurs qui s'y trouvent. En général, un canal est consacré à un sujet déterminé. Celui qui l'a créé est reconnu comme son «fondateur» et a le pouvoir d'en modifier les propriétés, d'en choisir les participants, d'en assurer la visibilité dans la liste des canaux publics du serveur, etc. Il peut aussi partager ce pouvoir avec d'autres utilisateurs en les ajoutant à la liste «AutoOp» (ou AOP, liste d'opérateurs autorisés). Toute personne figurant sur cette liste peut expulser un utilisateur du canal, voire l'en bannir pour de bon, quelle qu'en soit la raison. À un niveau plus élevé de la hiérarchie se trouvent les IRCops (opérateurs IRC), qui dirigent le serveur et ont le pouvoir de chasser quelqu'un non seulement d'un canal en particulier, mais aussi du serveur lui-même. Les IRCops peuvent aussi modifier la configuration des canaux et exercent beaucoup d'autres fonctions administratives. Normalement, un serveur IRC compte de nombreux opérateurs de canaux et seulement une poignée d'IRCops. Pour ces derniers, une intervention dans une querelle interne est généralement perçue comme une tâche ingrate, car elle leur demande de porter un jugement sur des événements qui leur sont étrangers. Par conséquent, les décisions relatives à un canal sont généralement confiées à ses opérateurs, et les IRCops n'interviennent que dans des circonstances exceptionnelles.

Les traces laissées sur IRC et les sites stables où l'on interagit permettent à de nombreux participants de trouver (ou à tout le moins de *chercher*) quelles sont les normes à respecter. L'ordre qui y règne est

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

néanmoins précaire, toujours au bord de basculer. Cependant, comme souvent pour tout ce qui implique des *tricksters*, ces moments de chaos ne sont pas nécessairement vecteurs d'échec ou de paralysie, ils jouent plutôt un rôle de déclencheur, lequel est essentiel à la vitalité de la société dans son ensemble, voire à sa régénération. La juxtaposition des deux citations suivantes, l'une du philosophe hispano-américain George Santayana et l'autre de Henry Brooks Adams, met cet enseignement en évidence: «La notion de chaos désigne tout ordre qui trouble l'esprit, mais celui-ci cesse d'être chaos aussitôt qu'on le perçoit comme tel[3].» «Souvent, le chaos engendre la vie, tandis que l'ordre engendre l'habitude[4].»

Le récit quelque peu sinueux que je m'apprête à livrer montre à quel point Anonymous reste perméable au hasard et au chaos, comme la plupart des mouvements sociaux. Mais le collectif se distingue sans doute des autres groupes par le fait qu'il est un tout petit peu plus ouvert à la mutation. Cette réceptivité sera démontrée de manière frappante début décembre 2010, alors qu'une décision saugrenue mettra fin à une période d'inactivité d'AnonOps, ouvrant la voie à de nouvelles perspectives d'action et permettant à des dizaines de nouveaux venus de se constituer en un véritable contingent d'appelés (ignorant pour la plupart, cette fois encore, l'existence du canal IRC semi-privé #command). La décision revitalisera AnonOps à un point tel que le réseau IRC du groupe deviendra une source intarissable d'activités pendant plus d'un an et surpassera même WikiLeaks comme plaque tournante du hacking activiste.

Mais avant de se pencher sur cette étrange décision, rappelons son résultat le plus notoire, à savoir le soutien qu'a apporté AnonOps à WikiLeaks par l'entremise d'une campagne massive d'attaques par saturation, dans la foulée de la fuite la plus controversée jamais communiquée par l'organisation des lanceurs d'alerte. Le 28 novembre 2010, en effet, WikiLeaks rendait publics 220 des 251 287 câbles diplomatiques classifiés dont elle disposait. Il s'agissait de la fuite de documents secrets la plus massive de tous les temps. Elle coïncidait avec la publication d'analyses en profondeur par *The Guardian*, *The New York Times*, *El País*, *Le Monde* et *Der Spiegel*. Le gouvernement américain vit

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

rouge. Trois puissantes sociétés soumises à son influence (Amazon, MasterCard et PayPal) cessèrent aussitôt de traiter les dons faits à WikiLeaks ou d'héberger ses sites web.

Bien que WikiLeaks eut déjà divulgué des centaines de milliers de documents militaires traitant des guerres en Afghanistan et en Irak, lesquels regorgeaient de révélations sur les opérations de capture menées par les forces spéciales, les victimes civiles, la prostitution de mineurs et toute une série d'horreurs du même ordre, le «Cablegate» relevait d'une catégorie à part. Cette fuite ne levait pas seulement le rideau sur les discussions protocolaires entre diplomates, elle le levait aussi sur leurs échanges internes parfois croustillants et sur leur travail de collecte de renseignements. En 2009, apprenait-on, Hillary Clinton, alors secrétaire d'État, avait fusionné la diplomatie et l'espionnage en ordonnant au personnel des ambassades et des consulats de récupérer les numéros de carte de crédit, les données de programmes «grands voyageurs» et les données biométriques de hauts responsables étrangers. On apprenait que l'administration Obama menait une guerre secrète au Yémen, où avaient lieu des tirs de missiles contre de présumés terroristes, des opérations couvertes par le gouvernement yéménite, qui en endossait la responsabilité. On apprenait que les agences de renseignement américaines croyaient que la Corée du Nord avait fait don à l'Iran de 19 de ses missiles de longue portée les plus puissants, dont le public ignorait jusque-là l'existence. On apprenait que le régime saoudien avait pressé les États-Unis de bombarder l'Iran afin de «couper la tête du serpent», pour reprendre les mots du roi Abdallah lui-même. Les câbles diplomatiques révélaient que le gouvernement israélien avait bluffé lorsqu'il avait menacé l'Iran de frappes aériennes, et que Washington avait effectué des transactions criminelles avec le frère du président afghan Hamid Karzai, un trafiquant de drogue véreux. Ils abordaient également des sujets plus triviaux, comme la médisance au quotidien des diplomates américains à l'égard des dirigeants étrangers[5]. Les fuites précédentes, guère captivantes, avaient à peine suscité la polémique. Cette fois, les révélations qui ont déferlé ont laissé le public bouche bée.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Sarah Palin recommanda de traquer Julian Assange «avec la même énergie que nous mettons à pourchasser Al-Qaïda et les chefs talibans[6]». Le sénateur Joe Lieberman qualifia la fuite de «geste scandaleux, irréfléchi et méprisable qui porte atteinte à la capacité du gouvernement et de ses partenaires à assurer la sécurité de la population et à collaborer à la défense de nos intérêts vitaux[7]». Son bureau contacta Amazon (qui, en plus d'être le plus gros détaillant de livres au monde, en est aussi le plus important hébergeur web) pour lui demander de bannir WikiLeaks de ses serveurs, ce qui fut accepté. Les sociétés financières qui traitent les transactions par carte de crédit à l'échelle mondiale lui emboîtèrent le pas en coupant le cordon entre WikiLeaks et ses donateurs. Bien qu'aucun tribunal n'ait jugé WikiLeaks coupable de quoi que ce soit, ces firmes, qui n'avaient aucune obligation juridique de faire ce que le gouvernement leur demandait, sont allées tout de même de l'avant. Ce qui a plongé les Anons dans une rage folle.

Deux semaines plus tard, AnonOps devenait l'épicentre de la campagne d'action directe la plus massive de l'histoire d'internet, du moins en ce qui a trait au nombre de participants (un record qui tient toujours). Plus de 7 000 personnes se connectaient au canal #operationpayback d'AnonOps pour donner un coup de main, applaudir ou tout simplement observer. Il s'agit du plus important rassemblement jamais vu sur un seul canal IRC[8]. Dans un texte d'opinion publié dans *The Guardian*, le célèbre hacker et militant pour le logiciel libre Richard Stallman qualifia l'événement de «manifestation de masse contre le contrôle[9]». En décembre seulement, Low Orbit Ion Cannon (LOIC) fut téléchargé 116 988 fois, soit nettement plus que lors des précédentes campagnes d'attaques par saturation[10]. Bien que seule une partie de ces téléchargements fût liée à la ruche d'Anonymous, l'intérêt pour l'outil fut manifestement alimenté par la couverture des activités du collectif.

Les médias, déchaînés, ont fait sortir le collectif de collectifs de l'ombre relative dans laquelle il était et l'ont propulsé sous les projecteurs de la scène mondiale. Le soulèvement ne fut pas seulement rapporté par les habituels magazines et blogs spécialisés en technologie, mais aussi par la

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

plupart des grands journaux télévisés. CNN accueillit l'expert en stratégie numérique Nicco Mele, qui fit l'éloge d'Anonymous lors d'une longue interview. Dans le *New York Times*, un des premiers saints patrons d'internet, John Perry Barlow, compara la campagne au «coup que le monde entendit», ce tir inaugural des batailles de Lexington et Concord célébré par Ralph Waldo Emerson[11].

WikiLeaks et Anonymous semblaient alors en parfaite harmonie, et cette alliance fut renforcée par le spectaculaire élan de solidarité et de soutien induit par la campagne d'Anonymous. Cependant, comme je l'ai laissé entendre précédemment, la décision d'intervenir avait été prise de façon assez désordonnée. Dans son essai intitulé *We Are Anonymous*, la journaliste Parmy Olson raconte qu'AnonOps n'y était pas allé par quatre chemins en choisissant de se rallier à WikiLeaks: «Les fondateurs d'AnonOps discutaient de l'affaire WikiLeaks sur leur canal privé #command. Ils étaient furieux contre PayPal, mais, plus encore, ils voyaient là une occasion d'agir. La victimisation de WikiLeaks, se disaient-ils, toucherait la corde sensible d'Anonymous et attirerait des hordes d'utilisateurs vers leur nouveau réseau. Une très bonne publicité[12].»

Mais cette interprétation reste superficielle. Car à l'époque, AnonOps fonctionnait au ralenti. Outre le noyau dur, le groupe n'avait pratiquement plus de sympathisants. Dans les faits, la prétendue «occasion d'agir» ne s'était pas présentée avant que les membres de #command ne se vissent *contraints* d'envisager une opération à la suite d'actions menées sur une base indépendante par quelques Anons inconnus, ce qui allait ouvrir la porte à des milliers d'autres.

On pourrait dire que l'étincelle qui a réveillé l'équipe de l'opération Payback en la précipitant dans l'opération Avenge Assange a jailli d'un flyer relativement verbeux où l'on chantait les louanges d'Assange: «Julian Assange vénère tout ce qui nous tient à cœur. Il méprise et combat infatigablement la censure [et] est sans doute le troll le plus brillant de tous les temps [...]. Julian est aujourd'hui la cible d'une chasse à l'homme planétaire, tant dans le monde virtuel que dans le monde réel.» On y invitait ensuite Anonymous à «riposter pour Julian» en menant diverses actions

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

politiques telles qu'attaquer PayPal ou envoyer des plaintes «au député de votre circonscription».

Le 4 décembre 2010, alors que ce message se répandait sur internet, un groupe non identifié lança une attaque par saturation contre le blog de PayPal, très probablement à l'aide d'un réseau de zombies[13]. La couverture journalistique de l'opération se révéla plutôt mince. Sur un ton laconique, le blog sécurité de PandaLabs (aujourd'hui Panda Security) annonça qu'AnonOps était impliqué: «Les organisateurs anonymes de l'opération Payback sont en train de réorienter celle-ci en vue de soutenir WikiLeaks dans son entreprise de divulgation de documents secrets de l'État[14].» Les Anons furent nombreux à tomber des nues. Alors que les reportages se succédaient, un débat houleux et alambiqué s'engagea sur #command, dont la plupart des membres ignoraient qu'ils étaient en train de «réorienter» leur campagne «en vue de soutenir WikiLeaks».

Pour bien comprendre cet épisode, il peut être utile de suivre quelques membres d'Anonymous au fil des événements du 6 décembre (tous les pseudos ont été modifiés). Nous commencerons par Fred, un des participants les plus influents de #command (selon un interviewé, Fred «est AnonOps»). Cet Anon consacrait beaucoup de temps à la maintenance de l'infrastructure – ce qui me fait songer à cet aphorisme de Kurt Vonnegut: «Autre défaut de la nature humaine: tout le monde a envie de construire, mais personne n'accepte de maintenir les choses en bon état[15].» Toujours disposé à accomplir des tâches que ses camarades tenaient pour acquises, Fred a fini par s'investir corps et âme dans AnonOps. Ce jour-là, au moment où il s'est connecté à #command, il était très en colère. La discussion qui aurait lieu au cours de l'heure qui suivrait changerait pour de bon la face d'AnonOps (en particulier) et celle d'Anonymous (en général).

<Fred> bordel
<Fred> cette opération assange, c'est juste un flyer
<Fred> pas de noms de sites, rien
<Fred> ça vient pas de nous

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Trogo, l'auteur du billet de blog de PandaLabs, était sur #command: il faisait partie des rares étrangers au groupe à qui l'on autorisait l'accès aux zones secrètes d'AnonOps afin d'y récupérer des informations à rendre publiques (et il était le seul «étranger» à être sur #command depuis sa création). Or c'était une publication de son cru qui semblait avoir incité bien du monde à prendre part aux actions dont on débattait à ce moment-là. Il défendit ainsi sa décision d'être allé de l'avant sans avoir attendu un consensus:

> <Trogo> [Elle avait été] approuvée par Radwaddie [un membre de #command]
> <Trogo> Nous avons procédé parce que le temps d'attention des médias est bref
> <Trogo> [à captor] Hier soir, j'ai écrit un billet de blog annonçant le changement dans les plans
> <captor> quel changement?

Des membres d'AnonOps avaient effectivement changé les plans, mais la plupart des Anons, y compris ceux de #command, n'avaient pas été conviés au processus de décision. Les exclus, prenant peu à peu conscience de la situation, furent nombreux à exprimer leur consternation. «On dirait qu'il y a bien du monde ici qui n'était pas au courant», écrivit Fred. Tandis que les reproches commencaient à fuser, d'autres Anons, interloqués, se disculpaient: «Ce n'est pas nous, nous n'avons pas attaqué PayPal.»

Tout étranger soit-il, Trogo entreprit alors de rappeler aux Anons un aspect fondamental du fonctionnement d'Anonymous: le nom peut être utilisé par quiconque le souhaite. Quelqu'un fit remarquer qu'il était ironique qu'il faille insister sur ce principe bien connu auprès, justement, d'Anons (et qui plus est, sur ce qui constituait sans doute le canal IRC d'Anonymous le plus important de l'heure). En plus de souligner ce qui relevait de l'évidence, Trogo, le chercheur en sécurité informatique, se justifia en affirmant que «rien de nouveau» ne venait de se passer, car il savait très bien que la plupart des membres du canal avaient déjà décidé

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

d’appuyer WikiLeaks, et ce, même si leur idée d’en faire un site miroir ne s’était pas encore concrétisée. Admettant l’impossibilité de revenir en arrière, Radwaddie troqua sa position défensive contre un discours plutôt offensif, tentant vigoureusement de convaincre ses camarades mécontents de profiter des circonstances pour foncer, c’est-à-dire pour attaquer PayPal sans s’attarder sur la stratégie déjà retenue:

> <Radwaddie> puisque nous sommes tous d'accord là-dessus [aider WikiLeaks]
> <Radwaddie> pourquoi pas attaquer paypal?
> <Fred> euh... parce que personne n'était au courant qu'on était censés le faire?
> <Radwaddie> écoutez, ça part déjà en couille, alors on pourrait aussi bien les aider

L’idée se révéla astucieuse. Les participants s’entendirent presque immédiatement sur la pertinence de se jeter dans la mêlée, même si certains d’entre eux insistaient pour qu’on procède en bonne et due forme. Pour ce faire, AnonOps devait activer sa machine de propagande. Par contre, au-delà du fait que l’idée d’attaquer PayPal en avait séduit plus d’un, la colère grondait de plus en plus (en particulier à l’endroit de Radwaddie et de Trogo pour leur mépris de la procédure décisionnelle):

> <dubiosdubious> [à Radwaddie] t'es qui toi pour prendre toutes les décisions?
> <Radwaddie> [à dubiosdubious] tu veux t'asseoir et discuter des prochaines opérations autour d'une tasse de thé?
> [...]
> <Radwaddie> [à dubiosdubious] c'est quoi ton objection (liste à puces stp)
> <dubiosdubious> 1. aucune préparation
> <dubiosdubious> 2. aucun vote
> <dubiosdubious> ce à quoi je pense d'emblée

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Tandis que Radwaddie tentait, malgré les attaques dont il faisait l'objet, de convaincre les autres de la nécessité de la campagne, une querelle sémantique éclata à propos du rôle de #command en général. Radwaddie s'emporta: «BORDEL DE MERDE, Y A PAS QUELQU'UN ICI QUI A UNE FOUTUE IDÉE?» Dans le même temps, l'idée faisait son chemin chez les Anons rassemblés sur #command, et le débat glissa lentement – et sans doute inévitablement – du caractère opportun d'une attaque sur PayPal à la composante même de PayPal qu'il serait opportun d'attaquer. La plupart des participants préconisaient le «site principal». Radwaddie proposa un mixte d'arguments pragmatiques et moraux: «On essaie de défendre une idée: on est en désaccord avec PayPal, [et c'est pourquoi] on opte pour ce qu'on fait le mieux, une attaque par saturation.» Il continua en rappelant qu'il s'agissait là de la raison d'être d'Anonymous, dont le rôle ne consistait pas à faire «de beaux discours» ou à bâtir «une communauté fabuleuse». Or, au moment même où la position de Radwaddie semblait sur le point de faire consensus, un participant appelé lark fit son entrée avec une information surprenante: «L'attaque [initiale] contre le blog de PayPal vient de nous; c'était un projet parallèle.» Ainsi, la toute première attaque par saturation, que les membres de #command attribuaient à quelque Anon non affilié, avait en fait été menée par un des leurs. J'imagine qu'il a tout simplement procédé discrètement, puisqu'AnonOps se consacrait alors essentiellement à la défense du partage de fichiers.

Néanmoins, malgré cette révélation, plus rien ne semblait pouvoir freiner l'élan d'AnonOps. Personne n'a daigné répondre à lark. Vu le bouillonnement induit par la décision de Trogo et de Radwaddie de tirer parti de la première attaque par saturation, cela peut paraître étonnant. Mais, à cette étape, les Anons étaient déjà dans le feu de l'action, si bien que l'intervention est sans doute passée inaperçue. Le débat poursuivit tout simplement son cours. Une annonce finit par survenir:

<captor> C'EST FAIT
<captor> nous avons une cible [le site principal de paypal]

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

L'équipe de propagande fut prévenue et l'attaque commença (avec le déploiement secret d'un réseau de zombies). La conversation dévia spontanément vers la nécessité d'élargir la portée de l'opération Payback (ici désignée par le sigle o:p) à d'autres enjeux que les droits d'auteur et le piratage:

> <Mobile> alors l'o:p s'est transformée en guerre contre la censure et le droit d'auteur?
> <Radwaddie> et nous considérons ça comme une opération parallèle, nous n'interrompons pas nos activités «normales»
> [...]
> <Trogo> Est-il seulement possible d'attaquer PayPal?
> <Radwaddie> [à Trogo] on verra bien, non?

Les Anons de #command ne le savaient pas, mais l'attaque qu'ils venaient de lancer n'était pas une simple «opération parallèle»: il s'agissait de la première salve d'un combat où prendrait forme un véritable mouvement planétaire, ouvrant une nouvelle ère pour Anonymous. Ce nouveau nœud, qui compterait des milliers de participants, ne naîtrait pas d'une volonté sans faille, mais plutôt d'une grande confusion, soit d'un joyeux mélange de manipulation, de fausses informations, de bonnes intentions et d'une large part de hasard.

Ils ne l'ont pas cherchée, ils ne l'ont pas choisie

La réponse à la question de Trogo («Est-il seulement possible d'attaquer PayPal?») s'est révélée positive. (MasterCard et d'autres sociétés financières connaîtraient d'ailleurs le même sort.) Assez rapidement, ce qui n'avait d'abord été conçu que comme un projet parallèle a mené AnonOps à son apothéose. Du 6 au 8 décembre 2010, le groupe élargit sa portée: au blog et au site principal de PayPal s'ajoutèrent les sites web du procureur général de la Suède (car la justice suédoise accuse Assange de viol et tente d'obtenir son extradition[16]), du sénateur américain Joe Lieberman, de

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Sarah Palin, de MasterCard, de Visa, d'EveryDNS (un gestionnaire de noms de domaine) et d'autres organisations. Exerçant sa vengeance contre quiconque était complice des préjudices causés à WikiLeaks, AnonOps bloqua tous ces sites pendant un certain temps (le nombre d'heures d'interruption varie selon qui en fait état). Le 8 décembre, le canal IRC public #operationpayback enregistra une fréquentation record de 7 800 participants.

Ces exemples montrent que les tactiques d'Anonymous correspondent à ce que Michel de Certeau interprète comme des «tactiques quotidiennes de résistance», où une «tactique dépend du temps, vigilante à y "saisir au vol" des possibilités de profit[17]». Radwaddie et Trogo avaient décidé d'agir indépendamment du groupe en saisissant précisément une occasion du genre, arrivée à point nommé; cette façon de prendre une décision, à la volée, est typique d'Anonymous. Le collectif agit plus souvent de façon réactive que proactive: pour paraphraser le poème mis en exergue en début de chapitre, *on leur a imposé la décision, ils ne peuvent la refuser, ils ne l'ont pas cherchée, ils ne l'ont pas choisie, mais il n'en tient qu'à eux d'agir.* Néanmoins, l'opération s'est avérée très exigeante sur le plan organisationnel et a nécessité des ressources considérables, qui ont pris la forme de réseaux de zombies, de *botnets* volontaires et de propagande.

Ce qui a fait la différence est à la fois simple et indépendant de la volonté d'Anonymous: l'indignation générale suscitée par le blocage des paiements à WikiLeaks. La consternation fut palpable dans le déferlement d'articles et de tweets où chacun reprenait à son compte cette question posée par un journaliste britannique sur Twitter: «De quel crime Assange ou WikiLeaks ont-ils été reconnus coupables pour que Visa, MasterCard, PayPal et Amazon interrompent leurs services cette semaine[18]?» Pour illustrer l'hypocrisie de toutes ces firmes, des gens soulignaient le fait que, pendant que MasterCard refusait de traiter les dons à WikiLeaks, les racistes du monde entier restaient libres de contribuer aux organisations de leur choix, tel le Ku Klux Klan. La sociologue spécialisée dans les questions relatives à internet Zeynep Tufekci fit cette mise en garde: «L'affaire WikiLeaks montre que ces institutions de pouvoir sont en train de

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

prendre le contrôle, lentement mais sûrement, des points charnières qui structurent le net. En tant que “sphère quasi publique”, internet est comparable aux centres commerciaux, ces endroits qui ressemblent à des espaces publics, mais où les droits des citoyens sont limités parce que ce sont en fait des endroits privés[19].»

C’est cette dure réalité qu’AnonOps était en train d’affronter: souvent perçu comme un lieu public, internet est un espace privé où les Amazon et autres PayPal de ce monde ont la capacité d’étouffer les débats et d’entraver le commerce.

Un activiste dont le nom d’utilisateur Twitter est AnonyOps (aucun lien avec AnonOps malgré la ressemblance) a bien décrit l’ambiance régnant alors dans certains milieux: «Une montagne de colère était en train de grandir en moi, et ce jour-là ça m’a frappé: il ne s’agissait pas d’une montagne, mais d’un volcan. Le jour où les dons à WikiLeaks ont été bloqués, le volcan a explosé, et je me suis mis à chercher un moyen de dénoncer toute cette merde. Un moyen de m’exprimer publiquement sans nuire à ma carrière[20].»

Ce riche ingénieur dans la trentaine a créé ce jour-là le compte Twitter AnonyOps (qui deviendra l’un des plus gros comptes à auteurs multiples d’Anonymous), puis, comme tant d’autres internautes, il s’est connecté à IRC.

AnonOps, plus proche de l’équipe bien dotée en bénévoles et en ressources que de la masse informe, avait bel et bien créé une plateforme permettant à toutes sortes de gens d’agir. Hasard et confusion s’y mêlaient à une bonne capacité opérationnelle et un solide déploiement de ressources. Une foule de citoyens sensibilisés, provenant de partout dans le monde, se mirent conséquemment à grossir les rangs de l’armée rebelle.

«Bonne nuit, faites de beaux rêves!
De la part d’AnonOps»

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

À l'automne 2010, alors qu'AnonOps multipliait les vagues d'attaques par saturation dans le cadre de l'opération Payback, j'étais en congé d'Anonymous en vue de terminer mon premier essai sur le hacking et le logiciel libre. J'avais pris du retard, et le compte à rebours qui menait à ma titularisation allait bon train. La pression était écrasante. Elle me tenaillait psychologiquement: pour conserver mon poste, je devais publier un livre. J'avais donc bloqué tout le mois de décembre pour le sprint final. Pourtant, quand Anonymous a refait surface au début du mois, j'ai fait confiance à mon sixième sens: l'événement aurait une trop grande portée historique pour que je passe à côté. J'ai donc mis mon manuscrit de côté pour concentrer mon attention sur Anonymous. Franchement, le pari ne me semblait pas risqué: connaissant les opérations antérieures du collectif, je me disais que celle-ci ne ferait pas long feu, ou à tout le moins s'essoufflerait au bout d'un mois, au terme duquel je pourrais me remettre à l'écriture. Mais, en fait, je finirais par passer les trois années suivantes enchaînée à mon ordinateur...

Vers la fin du mois, donc, je me suis rendue sur la côte Ouest pour passer les Fêtes avec ma famille. Pendant que mes proches partaient en randonnée sur les falaises accidentées qui surplombent le Pacifique ou regardaient des films jusque tard dans la nuit, je restais scotchée à mon portable. J'étais totalement absorbée – que dis-je? abasourdie, stupéfaite et tout bonnement accro à l'énergie brute et à la frénésie qui circulaient sur les canaux. Non sans raison, les membres de ma famille jugeaient sans doute mon comportement comme intentionnellement antisocial. J'étais sans conteste l'égoïste du groupe, toujours moins prompte que les autres à embrasser l'esprit des Fêtes – avec son lait de poule et, surtout, ses jeux de société, qu'ils adoraient autant que je les détestais. Chaque année, j'avais une demi-douzaine d'excuses toutes prêtes au cas où quelque signe laisserait présager l'imminence d'une partie de *Colons de Catane.*

Pour la plupart des membres de ma famille, internet, c'est la corvée des courriels à trier, les nouvelles qu'on lit en buvant son café du matin, le coup d'œil sur sa page Facebook pour voir les dernières photos des amis (et

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

de leurs bambins) et, dans les moments d'ennui mortel au travail, le visionnage de fantastiques vidéos de chats. Pour moi, internet représente les mêmes choses, mais aussi beaucoup plus: c'est un lieu où cohabitent une multitude de mondes, une véritable galaxie. Pour eux, il ne s'agit pas d'un «lieu» où un événement comme les manifestations contre l'Organisation mondiale du commerce (OMC), qui ont pris Seattle par surprise à la fin du siècle dernier, peut se produire. Et il y a indubitablement un océan de différence entre le gaz lacrymogène et les touches d'un clavier. Néanmoins, ces dissemblances mises à part, une chose me semblait sûre à ce moment-là: j'étais témoin de la première grande manifestation populaire en ligne, et je n'allais la rater pour rien au monde, *surtout pas* pour les *Colons de Catane*.

Après une longue journée de recherche, je ne demandais pas mieux que de décrire à ma famille les scènes marquées par le tumulte et l'enthousiasme qui s'étaient déroulées sous mes yeux. Mais les mots me manquaient. Pendant des semaines, je m'efforcerais de saisir ce qui se passait et de définir le type de «manifestation de masse» qui avait cours. Plutôt que des réponses, des questions me venaient à l'esprit. *S'agissait-il de désobéissance civile? d'action directe? d'un genre de manifestation de rue? d'un sit-in virtuel? d'un blocage? Les attaques par saturation brimaient-elles la liberté d'expression et d'autres droits fondamentaux, comme le prétendaient des voix critiques? L'opération respectait-elle l'éthique? Était-elle efficace? Et qui étaient donc tous ces gens?*

Au début, je n'en avais qu'une vague idée. Les pseudos déferlaient sur IRC. Un peu plus tard, je chatterais sans cesse avec certains Anons, et je finirais par en rencontrer quelques-uns en personne. Mais pour le moment, ces gens étaient pour moi de véritables mystères. J'ignorais tout de l'existence des canaux secrets; pour l'essentiel, je suivais les discussions qui se déroulaient sur #operationpayback et d'autres canaux publics. J'ai dû me familiariser avec le fonctionnement de LOIC et faire des recherches sur les attaques par saturation menées par AnonOps au cours de l'automne. La cadence effrénée de l'opération et le nombre considérable de participants faisaient paraître insignifiantes toutes les autres conversations sur IRC dont j'avais été témoin. Et même si je dépensais très peu d'énergie sur le plan

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

physique (je restais assise à suivre des discussions), je terminais invariablement mes journées épuisée, affligée d'un solide mal de tête, la conscience déchirée quant au jugement à porter sur les événements. Il me faudrait quelques semaines encore pour saisir l'éthique sur laquelle Anonymous fondait ses attaques par saturation.

Les participants devaient traiter une quantité d'informations ahurissante. Sur le canal principal, une fenêtre affichait d'abord le sujet et un résumé des données relatives à la cible: l'adresse IP à entrer dans LOIC, les canaux Twitter à consulter pour se familiariser avec le contexte, et une liste d'autres canaux IRC à aller voir. En général, le contenu était présenté comme ceci:

> (04:56:18) Le sujet de #opb est: OPÉRATION PAYBACK "http://anonops.eu/" http://anonops.eu/| Twitter: "http://twitter.com/Op_anon" http://twitter.com/Op_anon| "http://www.justiceforassange.com/" http://www.justiceforassange.com/Hive: 91.121.92.84| Cible: "http://www.mastercard.com/" www.mastercard.com| Voir: #Setup #Target #WikiLeaks #Propaganda #RadioPayback #Protest #Lounge et /liste pour le reste| "http://808chan.org/tpb" http://808chan.org/tpb

Sans relâche, Anonymous produisait flyers, vidéos et manifestes bien argumentés. Le collectif puisait dans un désenchantement profond et généralisé, et, en offrant un véhicule à l'activisme de confrontation, il donnait à celui-ci une forme plus visible et plus cohérente. C'était comme si tout le monde était conscient d'être en train d'écrire l'histoire, celle du premier soulèvement populaire sur internet. De parfaits inconnus s'unissaient les uns aux autres pour atteindre un but commun. J'étais moi-même dans un état d'exaltation absolu.

Il en allait tout autrement des discussions. Avec des milliers de personnes connectées et jusqu'à 100 utilisateurs qui s'exprimaient en même temps, il régnait une cacophonie épouvantable; pour la suivre, je devais mobiliser jusqu'au dernier neurone de mon cerveau de TDAH. D'ailleurs,

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

sans doute aucun support n'est plus propice que l'IRC à ce que le théoricien de la littérature Mikhaïl Bakhtine appelait la «polyphonie» (où s'exprime une multitude de voix, chacune ayant sa propre perspective et son propre poids moral)[21]. Et, bien que d'aucuns qualifient Anonymous de «microcosme de l'anarchie, dépourvu de morale, d'empathie et de programme[22]», ce qui se déroulait sous mes yeux était bien différent: chaque participant prenait position sur le plan moral et avait une raison de s'engager dans l'opération. Les gens se sentaient concernés, avaient soif de justice, souhaitaient mettre fin à la censure (certains s'opposaient même avec véhémence aux tactiques employées). Alors oui: Anonymous n'avait pas de programme universel en tant que collectif, mais les participants, eux, étaient guidés par leurs propres boussoles morales, bien réglées.

Citons un exemple parmi les dizaines d'enjeux ayant fait l'objet de discussions enflammées. En décembre 2010, #operationpayback fut le théâtre d'un débat virulent sur l'efficacité et la dimension éthique de la contestation technologique en général et de l'attaque par saturation en particulier. Deux aspects sont sortis du lot: la sécurité de LOIC et la question, plus philosophique, de savoir si l'attaque par saturation était un acte de liberté d'expression ou un acte visant à priver autrui de ladite liberté. Les deux discussions, dont voici des extraits, témoignent du caractère polyphonique de ces échanges et des multiples positions éthiques qu'inspirent ces formes technologiques de protestation. Ces enjeux ont été débattus et rebattus tout au long du mois.

Tôt dans la campagne, les participants se querellèrent sur la portée politique réelle des actions d'Anonymous. La plupart d'entre eux appuyaient le recours aux attaques par saturation:

<P> c'est mieux que l'OMC à Seattle
<P> une stratégie qui part de la base
<z> mais on a besoin d'une masse critique pour inspirer les gens
<z> 2 ou 3 personnes qui manifestent, ça en jette pas trop, ça a l'air foireux
<a> l'attaque semble assez désorganisée pour le moment

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<z> ça va devenir viral, vous savez
<P> le message est assez séduisant, je trouve
<a> je pense que le but des attaques est moins de nuire aux entreprises que d'attirer l'attention pour forcer les médias à couvrir l'affaire
<a> la plupart des gens que je connais ne savaient rien de WikiLeaks avant que je leur en parle
[...]
<a> D'après moi, l'attaque par saturation est la manière la plus efficace de protester en se servant des nouvelles technologies. Tant que la liberté d'information n'est pas totale, il n'y a pas de raison d'arrêter.
[...]
<m> il n'y a rien de mal à protester par les technologies, à part qu'on galère à s'organiser et à faire vraiment des dégâts. Et il n'y a pas beaucoup de bons hackers parmi nous.
<P> publications twitter et facebook synchronisées, pavillons pirates à poster un peu partout sur le net, et manifeste expliquant comment occuper le coin de sa rue pour faire quelque chose
[...]
<P> anon peut faire bouger les choses, mais ça, c'est plus gros qu'anon

Quelques jours plus tard, sur le même canal, quelques participants pourfendaient l'attaque par saturation tandis que les autres continuaient de la défendre:

<26> je pense pas qu'on puisse justifier une attaque par saturation au nom de la liberté d'expression
<26> parce que son but est de faire taire
<matty> ^
<sc> imaginez que la cible est une enseigne sur un immeuble
<secreta> pour moi, c'est très hypocrite, une attaque par saturation

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> <PN> t'arrêtes pas de crier que tout le monde ira en prison. t'es juste ici pour nous décourager. connard.
> <sc> t'es pas d'accord avec ce que cet immeuble représente
> <26> mais des gens vont en taule
> <ri> N'AYEZ PAS PEUR DE LA TAULE
> [...]
> <ri> dans toute campagne de protestation pour les droits civils, des gens finissent en taule

On peut présumer que la grande majorité des utilisateurs de LOIC considéraient cet outil et la tactique qu'il servait comme moralement acceptables. La *légalité* de LOIC, elle, était une tout autre question. Selon la ligne de parti alors défendue par AnonOps, LOIC était un moyen sûr de procéder à une attaque par saturation, non pas parce qu'il permettait à son utilisateur de masquer son adresse IP (il ne le permettait pas, et personne ne le prétendait), mais parce que, avec un très grand nombre de participants, il était pratiquement impossible – ou à tout le moins extrêmement difficile – pour les autorités de traquer et d'arrêter tout le monde. En de très rares occasions, il était arrivé que les principaux administrateurs du canal #operationpay back, dont certains faisaient aussi partie de #command, bannissent un participant ayant osé mettre les autres en garde contre l'illégalité de LOIC: les membres de #command souhaitaient que leurs méthodes inspirent la confiance, et non la crainte. AnonOps avait aussi fait circuler un «mode d'emploi» de LOIC qui contenait des recommandations grotesques en matière de sécurité et un conseil juridique insistant – et carrément douteux – à suivre en cas d'arrestation:

> SI ON VOUS EMBARQUE, déclarez que vous n'avez pas participé. Rappelez-vous que vous avez une adresse IP dynamique, utilisée par de nombreuses personnes justement à cause de sa nature dynamique. Si on prouve qu'une des adresses utilisées était la vôtre, dites que vous avez été victime d'un «virus *botnet*» dont vous ignoriez l'existence et sur lequel vous n'aviez aucune prise. De plus, si votre routeur sans fil n'était pas sécurisé ou l'était par WPA avant que vous n'utilisiez

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> LOIC, vous pouvez affirmer que quelqu'un a piraté votre connexion wi-fi. Affaire classée[23].

Chose plus grave, un petit groupe de journalistes avait aussi répandu de fausses informations. Si les erreurs d'Anonymous sont sans doute compréhensibles et pardonnables, les journalistes, eux, auraient du faire leurs devoirs au lieu de relayer les mauvais conseils juridiques et les recommandations techniques trompeuses de leurs sources. Le 8 décembre 2010, le populaire site d'information technologique *Gizmodo* a en effet offert l'exemple le plus frappant d'une telle négligence dans un article intitulé «What Is LOIC?» (Qu'est-ce que LOIC?): «En général, parce qu'une attaque par saturation met l'ensemble d'un site hors ligne, les fichiers journaux qui conservent normalement les traces de chaque connexion entrante ne fonctionnent plus[24].» Cette affirmation est carrément fausse. Le site attaqué peut continuer à surveiller son trafic, ce qui lui permet de conserver les adresses IP qui pourront éventuellement servir à incriminer des participants.

La sécurité de LOIC était digne de celle d'un préservatif troué. Quiconque utilisait ce programme sans avoir fait le nécessaire pour masquer son adresse IP pouvait être sûr que celle-ci apparaîtrait distinctement dans chaque paquet transmis (les «munitions» de l'attaque). Or de nombreux participants ignoraient les rudiments de cette technologie, lesquels étaient pourtant essentiels à toute décision éclairée en la matière. Tant les journalistes que les participants se sont laissés emporter par l'excitation et berner par un sentiment de sécurité prédominant. Néanmoins, si naïve que se révéla leur position après coup, la plupart des membres de #command croyaient sincèrement que les participants étaient protégés par la force du nombre. Certains d'entre eux ont d'ailleurs utilisé LOIC et ont fini par se faire arrêter.

Ainsi, pendant l'essentiel de l'automne 2010, les Anons ont lancé des attaques par saturation sans en subir les conséquences, ce qui a alimenté chez eux un faux sentiment de sécurité. Ce dernier a volé en éclats lors des premiers raids du Federal Bureau of Investigation (FBI), fin décembre. En

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

fait, quand un internaute se joignait à la ruche d'AnonOps pour envoyer des paquets à une cible, ceux-ci incluaient un message personnalisé: «Bonne nuit, faites de beaux rêves! De la part d'AnonOps.» C'est ce qui a permis aux autorités de contester la défense de suspects qui prétendaient avoir «été victimes d'un "virus *botnet*"». Certes, un bon avocat aurait pu tailler cet argument en pièces, car le message pouvait très bien faire partie du virus (mais le problème, c'est que les bons avocats coûtent cher). Quoi qu'il en soit, ces enjeux n'ont fait l'objet d'aucune discussion sur les canaux. Ils n'ont même pas semblé compris.

Mais le vent a rapidement tourné. Peu après la première vague d'attaques, un flyer prévenant les participants des failles de sécurité de LOIC a commencé à circuler. Aux mauvais conseils donnés par des sites comme *Gizmodo* succédèrent, sur des sites comme *Boing Boing*, des articles fouillés qui incluaient mises en garde et analyses techniques détaillées des vulnérabilités du logiciel. À peu près au même moment, un programmeur de talent réunit une équipe d'Anons en vue d'entreprendre le codage d'une version plus sûre, mais plus difficile d'utilisation, de LOIC. Une fois celle-ci mise en ligne, elle fut téléchargée en masse, jusqu'à ce qu'on découvre... qu'elle contenait un cheval de Troie.

Fin décembre, la preuve irréfutable de la traçabilité des attaques a fini par se manifester: un peu partout aux États-Unis, des policiers à l'uniforme bleu foncé orné des lettres jaunes F, B et I firent des perquisitions dans plus de 40 demeures, où ils saisirent des disques durs bourrés de données incriminantes. En juillet 2011, le FBI arrêta 14 présumés participants; en octobre 2013, un grand jury en accusa 13 d'avoir pris part aux attaques menées dans le cadre de l'opération Avenge Assange et d'une partie de l'opération Payback. Ils ont plaidé coupable[25].

Après le raid du FBI, plus personne n'ignorait que LOIC ne répond pas aux normes de sécurité élémentaires, que les autorités américaines avaient envisagé de sévir contre les protestataires en ligne, y compris contre ceux qui n'utilisaient pas le programme (certains participants ont été inculpés sur la base de discussions IRC journalisées), et que la force du nombre n'était garante d'aucune immunité. Les Anons venaient de recevoir une dure leçon.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

L'attaque par saturation et sa morale tortueuse

Armé de ces connaissances, quels enseignements peut-on tirer des actions directes extraordinaires menées dans le cadre de la plus grande campagne politique d'attaques par saturation jamais vue sur le web? À l'automne 2010, cette tactique politique était déjà bien établie chez les hackers activistes; à cet égard, Anonymous n'a rien inventé. Dans les années 1990 et au début des années 2000, par exemple, l'Electronic Disturbance Theater (EDT, théâtre de perturbation électronique) avait mené des campagnes d'attaques par saturation désignées sous le nom de «sit-in virtuels», où se combinaient interventions techniques, poésie douteuse et performance. EDT s'en était pris aux sites web de l'État mexicain pour sensibiliser la population à la lutte des zapatistes pour l'autonomie au Chiapas[26]. Ses activistes avaient diffusé un communiqué de presse avant l'action et, même s'ils n'avaient attiré que quelques centaines de participants et n'avaient fait subir aucune interruption aux sites visés, ils étaient parvenus (jusqu'à un certain point) à retenir l'attention des médias. Quoi qu'il en soit, comme l'a observé Molly Sauter avec perspicacité, cette campagne n'aurait guère pu être qualifiée de «perturbatrice» et n'a jamais atteint un point de saturation dans les grands médias[27].

Là où Anonymous a innové, c'est dans l'échelle, le mode d'expression et les effets des attaques par saturation, à tel point que le collectif a brisé le moule dont il avait hérité. Au lieu de passer des mois à organiser soigneusement des événements d'envergure modeste, les Anons ont expérimenté, en temps réel, l'art de canaliser l'indignation pour la muer en un soulèvement indocile, imprévisible et continu. Comme dans toute assemblée publique, aux côtés de participants animés de préoccupations politiques s'en trouvait d'autres qui ne faisaient que suivre le mouvement et d'autres encore qui cherchaient à rendre l'aventure la plus mouvementée possible. Vu la doctrine philosophique et l'accessibilité des outils logiciels du collectif, il était inévitable que ses membres adoptent une panoplie de

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

positions et d'objectifs, et que leurs actions soient ouvertes aux activistes expérimentés comme aux nouveaux venus.

En l'envisageant dans une perspective historique, on constate que la tactique de l'attaque par saturation n'a rien de nouveau: pratiquement tous les mouvements qui ont lutté pour le changement social au cours des deux-cents dernières années (des anti-esclavagistes à Act Up) ont fait appel à des tactiques qui avaient pour but de déranger et de perturber à grande échelle pour attirer l'attention et faire valoir leurs revendications[28]. L'innovation, ici, réside plutôt dans la façon dont la disponibilité d'un logiciel, LOIC, et la promotion qui en a été faite par la machine de propagande d'Anonymous ont rendus possibles l'organisation et le déploiement quasi spontanés de manifestations d'une ampleur et d'une efficacité impressionnantes sur internet. Dans son analyse des caractéristiques de LOIC, Sauter affirme de manière convaincante que le «mode ruche» a permis l'afflux d'un grand nombre de participants: «Les Anons n'ont pas "pris la rue" comme l'aurait imaginé EDT, mais le mode ruche leur a permis de continuer à étudier, à travailler, à dormir ou à faire quoi que ce soit d'autre tout en participant aux attaques par saturation le moment venu[29].»

Toutefois, même si l'attaque par saturation s'inscrit dans une longue tradition d'activisme par la perturbation, nombreux sont les Anons et les hackers qui s'en accommodent difficilement, y compris parmi ceux à qui la désobéissance civile ne pose aucun problème. Pour un hacker d'Anonymous avec qui j'ai discuté de la dimension morale des campagnes de protestation, «quiconque tente de trouver une justification éthique infaillible à nos attaques par saturation s'expose à devoir faire des contorsions morales». Beaucoup d'Anons ont été estomaqués en apprenant que les campagnes de l'hiver et de l'automne 2010, dont l'opération Avenge Assange, avaient été lancées dans la duplicité et menées grâce au déploiement de *botnets* contrôlés par des hackers. S'ils avaient su que les munitions étaient fournies par une armée d'ordinateurs zombies, peut-être auraient-ils fait d'autres choix.

Et pourtant, sans l'importante contribution des ordinateurs détournés, le recours à LOIC (même par des milliers de participants convaincus et

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

mobilisés) n'aurait jamais pu provoquer les interruptions qui ont attiré l'attention des médias. Le hacker avec qui j'ai parlé, qui désapprouve la technique, précise: «J'ai souvent discuté des attaques par saturation avec des gens qui, comme moi, n'en sont guère friands, et nous finissons toujours par y revenir, car elles sont efficaces: les médias, eux, en sont friands.»

C'est là un aspect crucial. Sur le plan technique, une large participation du public n'était sans doute pas nécessaire, et les affirmations relatives à la sécurité de LOIC étaient complètement à côté de la plaque, mais, sans une masse critique apparente, l'opération aurait fort probablement été perçue comme manquant de sérieux et d'autorité morale. Même si elle ne garantissait pas la sécurité des participants (et qu'elle n'était pas techniquement indispensable), la force du nombre s'est avérée porteuse d'un puissant message: elle a concrètement révélé à la face du monde l'ampleur du désenchantement de ces activistes face à ce qu'ils percevaient comme un acte de censure perpétré par de grandes entreprises.

Des geeks et d'autres observateurs ont aussi soulevé des objections plus générales contre l'attaque par saturation en tentant de la comparer à ses équivalents du monde réel. La critique qui revenait le plus souvent était que les attaques bafouent le droit des cibles à s'exprimer librement. En envisageant la liberté d'expression dans son sens absolu, on peut effectivement considérer qu'une attaque par saturation anéantit une possibilité d'expression en bloquant l'accès à un site web qui contient un ensemble d'énoncés. Cet argument rejoint la position de certains hackers. Oxblood Ruffin, de l'association Cult of the Dead Cow, s'oppose à la tactique depuis des décennies: «Anonymous se bat pour la liberté d'expression sur internet, mais le groupe peut difficilement défendre cette position tout en menant des attaques par saturation qui empêchent des gens de s'exprimer. Où est la cohérence[30]?»

Il a raison, mais jusqu'à un certain point seulement. Une conception plus dynamique de la liberté d'expression devrait tenir compte des rapports de pouvoir. Parce qu'elle permet à des opprimés de s'exprimer aussi fort que leurs opposants mieux nantis (de puissantes sociétés, dans le cas qui

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

nous occupe), l'attaque par saturation peut être considérée comme un outil de nivellement, un moyen de faire progresser la liberté d'expression. Cette dernière, selon moi, doit donc être analysée dans son contexte, en fonction des rapports de force. Dans le cadre de l'opération Avenge Assange, PayPal et ses semblables n'ont jamais vraiment été privés de leur capacité de s'exprimer, et la campagne avait elle-même été lancée en réaction à un blocage unilatéral des dons et de l'hébergement web qui compromettait les possibilités d'expression de WikiLeaks. Alors que WikiLeaks ne disposait que d'un seul lieu d'expression (son site web mis hors service, auquel s'ajoutait parfois quelque journaliste sympathique à sa cause), la plupart des cibles d'Anonymous, telles la Motion Picture Association of America (MPAA) et PayPal, avaient à leur solde une armée de lobbyistes et de publicitaires – sans parler de leurs contacts dans les médias –, tous en mesure de faire rayonner leur message.

Néanmoins, comprendre l'attaque par saturation comme un modulateur de liberté d'expression semble en soi discutable. Des observateurs rapprochent plutôt cette tactique d'une autre action directe traditionnelle: le blocage. Lors d'un débat entre membres du Cult of the Dead Cow, le hacker Tod Gemüse a qualifié le lien avec la liberté d'expression de «foutaise»: «[L'attaque par saturation] est l'équivalent numérique de modes de contestation concrets comme le verrouillage des portes d'une usine ou le blocage de l'entrée d'un immeuble[31].» Les personnes qui critiquent la tactique au nom du fait que les entreprises ont dû investir dans la défense de leurs sites web ignorent tout de la nature de l'action directe. L'action directe va au-delà des notions politiques de discours, d'expression et de retentissement médiatique, car elle a pour but de nuire à l'organisation visée en interrompant ses activités[32]. L'attaque par saturation correspond effectivement à cette définition.

Bien sûr, ces arguments ne justifient pas le recours à l'attaque par saturation en toutes circonstance. Ils permettent plutôt de mieux saisir qu'elle relève d'une logique tortueuse et d'une éthique dépendant du contexte. Avec son équipe, le sociologue des médias et spécialiste d'internet Ethan Zuckerman a démontré à quel point une attaque par saturation peut

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

nuire à une petite organisation dépourvue des ressources d'une grande société[33]. Ainsi, même si l'on pouvait cautionner ce type d'attaques dans des cas ponctuels (disons, uniquement contre les organisations puissantes et bien équipées), leur éventuelle prolifération pourrait vite dégénérer en une «course aux armements», où les organisations disposant d'une large bande passante auraient le dessus sur celles qui n'en disposent pas.

Quoi qu'on pense de l'utilité et de la moralité de la tactique, on peut la comprendre un peu mieux en se penchant sur ses conséquences concrètes sur les plans technique et judiciaire. On sera ainsi mieux en mesure de soupeser l'équité (ou l'iniquité) des châtiments infligés aux participants. Contrairement à ce qu'on a pu lire ou entendre dans certains reportages, nul hacker ne s'insinue dans les serveurs qui font l'objet d'une attaque par saturation, et ceux-ci ne subissent ni dommages ni pertes de données[34]. Si l'organisation cible doit assumer des coûts, c'est avant tout parce qu'elle doit retenir les services d'une firme spécialisée dans la protection contre les attaques. Une attaque réussie bloque l'accès à un domaine. Elle peut empêcher les transactions commerciales électroniques, mais reste sans effet sur le système informatique interne de l'entreprise touchée. La forme d'attaque par saturation la plus communément menée par Anonymous, connue sous le nom de *traffic flood* (afflux de trafic), ne peut rien contre les sites de services où s'échangent beaucoup de données et qui font appel à des réseaux de diffusion de contenu (on utilise le signe anglais, CDN), comme c'est le cas d'Amazon.com. (Pendant une brève période, AnonOps a essayé de s'en prendre directement à Amazon.com, une tentative qui s'est soldée par un échec.) Même quand des milliers de personnes ont inscrit leurs ordinateurs dans un *botnet* volontaire, leurs efforts n'ont pas suffi à venir à bout de réseaux d'infrastructure comme Amazon Web Services. Les attaques d'Anonymous ont tendance à mieux réussir lorsqu'elles visent des sites d'information comme mpaa.org. Elles bloquent essentiellement l'accès à ces domaines, mais uniquement du côté de leurs sites web, qui donne sur internet.

Vu les conséquences d'une attaque par saturation, et quoi qu'on pense des risques et du sérieux d'une telle opération, une chose est sûre: les

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

accusations portées contre les membres d'Anonymous aux États-Unis et au Royaume-Uni sont sans commune mesure avec le caractère non violent des actes commis. Aux États-Unis, les arrestations consécutives à des attaques par saturation ont été menées en vertu de la Computer Fraud and Abuse Act (CFAA, loi sur la fraude et la malveillance informatiques), qui tend à induire des peines plus lourdes que celles qui découlent de lois comparables s'appliquant au monde tangible. En effet, hors ligne, des tactiques comme l'empiétement sur une propriété privée ou le vandalisme (qui provoque des dommages concrets) entraînent rarement des représailles judiciaires catastrophiques pour les activistes qui les pratiquent. Les actions menées en ligne, elles, bénéficient rarement du discernement d'un juge qui tiendrait compte de l'intention visée et des conséquences réelles, en particulier lorsque la CFAA est invoquée. Par conséquent, un comportement qui, hors ligne, vaudrait au contrevenant une condamnation pour délit mineur (assortie d'une amende ou d'une peine allant jusqu'à trente jours de prison) lui vaut une condamnation pour acte criminel grave (assortie d'une amende salée et d'une lourde peine de prison) s'il a été commis en ligne.

Au Wisconsin, par exemple, un camionneur âgé de 38 ans, Eric J. Rosol, a été mis à l'amende pour avoir utilisé un outil d'attaque par saturation automatisé contre le site web de Koch Industries pendant soixante secondes. (Dans le cadre d'une opération d'Anonymous, il dénonçait l'appui des frères milliardaires Koch au gouverneur de l'État dans ses efforts pour réduire le pouvoir des syndicats et limiter le droit de négociation collective des employés du secteur public.) L'attaque a occasionné une perte de 5 000 dollars à l'entreprise, mais Rosol a été condamné à 183 000 dollars d'amende – même si un délit physique autrement plus grave, l'incendie criminel, n'est punissable que de 6 400 dollars d'amende au Wisconsin[35]. Le montant de l'amende équivaut à la somme dépensée par les frères Koch pour les services d'une firme de consultants embauchée avant l'opération pour en minimiser les effets. Au Royaume-Uni, Chris Weatherhead, qui n'avait pas directement contribué à une campagne d'attaques par saturation, mais gérait le centre de communications où Anonymous avait coordonné celle-ci, s'est vu infliger

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

une peine de dix-huit mois de prison après avoir été «reconnu coupable d'un chef d'accusation de conspiration en vue de nuire au bon fonctionnement d'ordinateurs[36]».

Les conséquences judiciaires subies par ceux et celles qui ont été arrêtés dans la foulée des attaques contre PayPal méritent qu'on s'y penche un moment. Grâce à d'excellents avocats et à une négociation de peine (non encore conclue), la plupart des 13 accusés n'ont été condamnés qu'à 5 600 dollars d'amende chacun et ont évité la prison. Malgré des accusations de crime grave, le juge effacera sans doute leurs casiers judiciaires s'ils respectent leurs conditions de probation. Deux d'entre eux passeront quatre-vingt-dix jours en prison pour éviter toute accusation de crime grave, et le sort d'un des accusés reste incertain[37]. Bien que leurs peines soient moins lourdes qu'on pouvait s'y attendre, les accusés ont tout de même traversé une épreuve épuisante et coûteuse et, parce qu'ils risquaient une condamnation pour crime grave, nombre d'entre eux ont eu des difficultés à trouver du travail (et en auront peut-être encore).

Toute l'affaire a aussi été marquée par le double discours d'une entreprise en particulier, PayPal, qui, en poursuivant des participants de l'opération Avenge Assange, a fait preuve d'une hypocrisie flagrante. (Notons que MasterCard et Visa n'ont pas entamé de poursuites.) En cour, les avocats de PayPal ont évalué les dommages subis à 5,5 millions de dollars[38]. Au même moment, en d'autres lieux, des cadres de la firme affirmaient que «PayPal n'a jamais cessé de fonctionner» ou que l'attaque avait simplement «ralenti notre système, mais si peu que nos clients ne s'en sont pas rendu compte[39]». Voilà qui montre très bien à quel point les acteurs des milieux d'affaires peuvent non seulement continuer à exprimer leurs points de vue à leur guise par une multitude de canaux, mais aussi tenir un double discours, comme le démontre le long et coûteux processus judiciaire imposé aux accusés.

Au sein d'Anonymous, le débat sur les attaques par saturation a fini par perdre sa raison d'être. On en est venu à mesurer l'efficacité de la tactique à l'aune de sa capacité à faire les manchettes. Le fait de dépendre de médias d'information obsédés par la nouvelle a conféré une demi-vie

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

très brève à la visibilité de campagnes comme Avenge Assange. Pas bêtes, les Anons voyaient venir cette évolution. Au moment de mettre fin à l'opération, le groupe a publié un flyer où il annonçait que, «au mieux, nous leur avons fait un œil au beurre noir. La donne a changé. Quand la donne change, nos tactiques doivent faire de même». À partir de décembre 2010, l'attaque par saturation, casse-tête moral non résolu, est devenue une arme brandie à l'occasion parmi un ensemble de tactiques de plus en plus diversifiées. Pendant ce temps, un petit pays, la Tunisie, était au bord de l'ébullition. Deux hackers, dont un membre d'AnonOps, déclencheraient des événements qui, une fois de plus, bouleverseraient l'existence du collectif de collectifs – des événements aussi déterminants que la naissance même de Chanology.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Chapitre 5

Anonymous Everywhere

ALORS QUE S'OUVRE L'ANNÉE 2011 et que l'opération Avenge Assange est sur son déclin, d'autres campagnes démarrent sur AnonOps. Loin de se fragmenter, le réseau Internet Relay Chat (IRC) est en plein essor. Les militants d'Anonymous de toutes tendances en ont fait leur plateforme de prédilection pour l'organisation de leurs opérations. Fin janvier, l'Italie, l'Irlande, le Venezuela, le Brésil, la Syrie, le Bahreïn, la Tunisie, l'Égypte et la Libye ont leurs canaux spécifiques, où sont lancées des campagnes. Des activités non associées à un lieu en particulier ont également cours, dont l'opération Leakspin (agitation liée à une fuite), qui consiste à passer au peigne fin les câbles diplomatiques divulgués par WikiLeaks pour y dénicher des informations croustillantes. Bien que modestes, ces efforts ont fait naître des nœuds régionaux dynamiques, les plus importants se trouvant en Italie, en Espagne, au Brésil et ailleurs en Amérique latine. (En 2013, par exemple, Anonymous Italie divulguera des documents issus du bureau du président de la Lombardie, qualifiant ce dernier de «gros enfoiré corrompu» et l'accusant, entre autres, d'avoir permis à des criminels qui distribuent de la pornographie juvénile de blanchir leurs fonds par l'entremise d'une banque lombarde[1].) Ces cellules locales prospèrent et deviennent de véritables communautés – mais rares sont celles dont l'activité est bien documentée[2].

L'opération Tunisie semble surgir de nulle part. Ce n'est que bien plus tard qu'on m'informera des circonstances précises de sa naissance; et son

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

fondateur cherchera ses mots lorsque je lui demanderai de m'en raconter la genèse: «Je ne sais pas trop pourquoi ça a marché.»

Deux geeks, Slim et Adnon (ce pseudo a été modifié), habitent deux régions différentes du monde et opèrent chacun de leur côté, tout en se retrouvant dans un même espoir de rendre le monde meilleur. Citoyen tunisien dans la trentaine, programmeur et blogueur, Slim Amamou est fasciné par le collectif de collectifs et aspire à ce qu'il contribue à faire connaître les crises qui secouent son pays. Dans ses conférences sur le pouvoir et l'attrait des mouvements politiques non identitaires, il compare Anonymous au nombre zéro, le nombre tout-puissant, le non-nombre. Venant d'un jeune Arabe ce rapprochement est éloquent: incarnant l'idée de vide et d'infini, le zéro vient de mathématiciens arabes et a longtemps été tenu pour un concept hérétique en Occident; il n'est pas entré dans l'usage de ses mathématiciens et philosophes avant le siècle des Lumières. Le zéro, marque substitutive par excellence, refuse toute identité concrète.

De l'autre côté de la Méditerranée, dans une pittoresque cité historique d'Europe, Adnon mène une existence privilégiée sans s'inquiéter de la répression; il a *choisi* l'anonymat d'Anonymous. Amamou, lui, est contraint à l'anonymat. La Tunisie est alors soumise à une censure sévère: en 2010, ce pays d'à peine plus de dix millions d'habitants occupe le 164^{e} rang sur 178 au classement mondial de la liberté de la presse de Reporters sans frontières (une évaluation annuelle de la liberté de presse fondée sur un questionnaire rempli par des ONG, des journalistes, des juristes, des universitaires et des défenseurs des droits de la personne de divers pays). Comme bon nombre de ses compatriotes, Amamou utilise des outils permettant de contourner la censure pour s'informer et faire circuler les nouvelles. L'utilisation de serveurs proxys et de réseaux privés virtuels (le sigle VPN*, provenant de l'anglais, est aussi utilisé en français) fait partie des «connaissances de base de la jeunesse», m'expliquera-t-il. En Tunisie, devenir un geek relève souvent de l'instinct de survie.

Très tôt, me racontera Amamou, Anonymous en vient à symboliser le ras-le-bol généralisé des Tunisiens. De jeunes hackers urbains et des paysans adoptent son imagerie, inspirés par le rôle que joue le collectif dans

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

la révolte qui balaye le pays. Bien des gens savent que c'est Anonymous qui attirera l'attention des médias, indifférents au début de la révolution. Le 8 janvier 2011, par exemple, une semaine avant la chute du président Zine el-Abidine Ben Ali, des écoliers s'assoient dans la cour de leur établissement et rendent hommage à Anonymous en revêtant le masque. Certes modeste et peu risquée, la contribution des Anons sera donc essentielle.

Déjà très actif politiquement sur internet, Amamou n'a pas toujours milité de façon anonyme. Le 21 mai 2010, des sbires du gouvernement l'ont arrêté parce qu'il participait à l'organisation d'une manifestation contre la censure du web prévue pour le lendemain devant le siège du ministère de l'Information. Le 6 janvier suivant, à l'apogée du mouvement de protestation, il est de nouveau arrêté. Du Japon à l'Europe, alors, des Anons ayant eu vent de son infortune (la nouvelle a circulé sur les canaux du collectif) submergent le gouvernement tunisien d'appels. «Les forces de sécurité m'ont interrogé pendant cinq jours, racontera-t-il. C'est un endroit où l'on tue les gens, voyez-vous, et je crois – non, en fait, je suis certain – qu'Anonymous m'a sauvé la vie.»

Ainsi, alors que son pays s'approche de plus en plus d'une véritable révolution, Amamou souhaite que le collectif sans visage s'engage davantage. Il pense que si une opération se met en branle, la presse mondiale ne pourra plus ignorer la Tunisie. Il appelle Anonymous à se manifester, mais il le fait sans illusion: il sait très bien qu'«Anonymous n'est pas votre armée personnelle». «Personne ne peut contrôler Anonymous», me rétorquera-t-il d'ailleurs, quand je voudrai savoir quelles transformations il apporterait au collectif s'il le pouvait. Tout ce qu'on peut faire, c'est espérer sa venue. Par chance, c'est ce qui se passera.

L'entrée en scène d'Anonymous est en partie attribuable à Adnon, qui est âgé de 15 ans au moment de sa découverte du collectif. Le jeune homme a grandi en Europe dans une famille très riche – chose impossible à deviner à première vue. Adnon a été un des premiers membres d'AnonOps que j'ai rencontré «afk» (*away from keyboard*, loin du clavier en jargon IRC), et j'ai eu souvent le plaisir de le revoir. De tous les Anons dont j'ai fait la

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

connaissance, il est le plus modeste. Gentil, calme et contemplatif, je l'ai d'abord pris pour un «type ordinaire», mais, au bout de vingt minutes, j'ai compris pourquoi certains hackers plus âgés se montraient affectueusement protecteurs envers lui.

Par une chaude journée d'été, à l'abri du soleil sous un arbre dont les feuilles nous bercent de leur bruissement, nous parlons donc d'Anonymous. En gros, notre conversation portera à 30 % sur les potins, à 20 % sur les conspirations et à 50 % sur les entrailles d'Anonymous, un exposé qui tombe à pic. La transition entre le chat en ligne et le dialogue en personne coule de source. C'est pour moi un véritable soulagement d'enfin rencontrer quelqu'un de ce milieu en chair et en os.

Adnon, qui se plaint de son boulot minable et ennuyeux (bien qu'il soit issu d'une famille riche, on ne l'a pas trop gâté), me raconte avec plus d'enthousiasme ses fréquentes excursions à vélo ou en canot. S'ennuyant parfois en classe, passant beaucoup de temps en ligne, il devient membre d'AnonOps à l'automne 2010, pendant la première phase de l'opération Payback. «J'ai décidé de m'impliquer après avoir lu un article quelque part; je me suis dit: "Wow, ils sont cools, ces hackers!" Mais c'était bien plus que ça.» Loin d'être un hacker de talent, il possède néanmoins de bonnes connaissances techniques; il se qualifie comme geek en bonne et due forme.

Embarquer dans le navire d'Anonymous lui permet d'acquérir de nouvelles compétences, dont la gestion de protocoles de sécurité, de bases de données et de serveurs web. Mais «les choses les plus importantes que j'ai apprises n'ont rien de technique, précise-t-il. Le travail d'équipe et l'organisation sont considérables». Il fait partie de ces organisateurs et intermédiaires (j'en ai rencontré quatre) dont Anonymous ne pourrait se passer pour faire tourner son horloge interne, un dispositif qui ressemble plus à une montre molle de Dalí qu'à une horloge suisse.

Pendant une bonne partie de l'automne 2010, Adnon fréquente le réseau IRC en spectateur avide, n'intervenant qu'à l'occasion dans les discussions relatives à l'organisation. Mais il chatte, en particulier avec des administrateurs de canal tels que joepie91. Vers la fin décembre, il lance une proposition, soutenue par les Anons avec qui il a été en discussion

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

pendant toutes ces longues heures. L'idée va changer le cours de l'histoire d'AnonOps.

La proposition d'Adnon est simple: utiliser les ressources d'Anonymous pour faire connaître la situation des Tunisiens en révolte contre leur président-dictateur Ben Ali, au pouvoir depuis 1987. «Nous avions un canal appelé #anonnews, où nous étions trois à faire les modérateurs. [...] Un des types, que je crois tunisien, a écrit quelque chose comme "Le type s'est immolé par le feu à cause de ça, et quelques petites manifestations ont eu lieu. Ce serait bien de faire quelque chose."» À ce moment-là, le gouvernement est déjà parvenu à bloquer l'accès aux câbles diplomatiques de WikiLeaks qui portaient sur la Tunisie, lesquels ont amené toute une cohorte de geeks à se solidariser dans l'urgence[3].

Au départ, certains participants au canal martèlent qu'il serait «insensé [...] de renverser un gouvernement». Adnon n'insiste pas. Une semaine plus tard, à la veille du Nouvel An, un soir de blizzard, alors que le jeune homme est en vacances en famille, il s'esquive en douce dans sa chambre d'hôtel pour se connecter au serveur IRC. Conforté par un sentiment de droiture – et par une certaine dose d'informations erronées et de mésinterprétation –, il décide de répliquer aux pessimistes. «Ignorant le nombre réel d'Anons *moralfags*, j'ai présumé que le groupe comptait des milliers de membres actifs, et j'ai lancé: "Pourquoi pas?"» Il est vrai que des milliers de personnes ont participé à l'opération Avenge Assange, mais l'effectif stable se chiffre alors plutôt en centaines, et les Anons qui se consacrent à la propagande et aux aspects techniques commencent à se faire rares. Mais Adnon tient bon et finit par convaincre un nombre suffisant d'Anons:

> <Adnon> À partir du canal #optunisia, on a fait suivre le lien partout
> <Adnon> les gens n'ont pas apprécié
> <Adnon> c'était une idée dingue

Parmi les adhérents, un grand nombre reste sceptiques, «peu convaincus que l'opération ou la révolution aient la moindre chance de succès», écrira

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Quinn Norton dans le magazine *Wired*[4]. L'opération sera pourtant la plus remarquable de l'histoire du groupe, qui, d'Anonymous, se transformera en *Anonymous Everywhere*. À partir de ce moment-là, le collectif ne se limitera plus aux enjeux liés à internet tels que la censure ou le partage de fichiers.

Un jour ou deux après avoir relancé sa proposition, Adnon reçoit sur IRC un message privé d'un membre de #internetfeds. De la part des participants au canal, celui-ci lui offre divers services: défaçage de sites web, attaques par saturation, intrusions... la tâche va-t-elle être plus facile qu'Adnon ne l'a cru? Le 2 janvier 2011, à l'aube de la nouvelle année (toujours signe d'espoir), Anonymous diffuse un communiqué de presse marquant le lancement de l'opération Tunisie, lequel sera bientôt traduit en français, en arabe, en espagnol et en italien:

> Le temps de la vérité est venu. Un temps où le peuple s'exprime librement et peut être entendu partout dans le monde. Le gouvernement tunisien veut contrôler le présent à l'aide de mensonges et de désinformation, son but est d'imposer l'avenir en dissimulant la vérité à ses citoyens. Nous ne resterons pas silencieux devant cette situation. Anonymous a entendu le cri de liberté des Tunisiens. Anonymous souhaite les aider dans leur combat contre l'oppression. Ce sera fait.
>
> Ce communiqué se veut un avertissement au gouvernement tunisien: nous ne tolérerons pas ses attaques contre la liberté d'expression et d'information de ses citoyens. Toute organisation se livrant à la censure sera visée et ne retrouvera pas la paix tant que le gouvernement tunisien ne répondra pas à son peuple, qui réclame la liberté. Il ne tient qu'à lui de mettre un terme à la situation. Libérez internet, et les attaques cesseront; persistez dans la censure, et elles ne feront que commencer.

Le tigre mange quatre poulets par jour

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Mais revenons au déclenchement de la révolution elle-même, dans lequel Mohamed Bouazizi, le blog *Nawaat*, WikiLeaks et Chelsea Manning ont tous joué un rôle.

C'est depuis 1987 que le régime de Ben Ali tient les Tunisiens sous son joug. Opprimés, soumis à des conditions de vie déplorables, ils vivent dans la crainte de la torture, de la censure et des détentions abusives – des violations des droits de la personne qui, en 2010, se multiplient. La Tunisie n'a pas été le théâtre de grandes manifestations depuis plusieurs décennies, et bon nombre de ses alliés occidentaux, dont les États-Unis, la citent comme modèle pour sa stabilité politique et économique dans un monde arabe autrement réputé pour ses conflits et son instabilité.

Quand la révolution éclate – et quand les grands médias décident *enfin* de la couvrir comme il se doit –, le choc ébranle le monde entier (du moins le monde occidental). Les manifestations font tomber la dictature – une des chutes les plus rapides de l'histoire récente – et provoquent une réaction en chaîne dans le reste de la région, inaugurant ce qu'on désignera sous le nom de Printemps arabe. Comme lors de tant d'épisodes révolutionnaires, constatera-t-on plus tard avec le recul, le désarroi cumulé était assez grand pour alimenter le brasier de la révolte pendant des semaines. Tout ce qu'il manquait, c'était une allumette. Et la Tunisie s'en est vu offrir deux.

Le 28 novembre, d'abord, quand WikiLeaks divulgue sa première série de 220 câbles diplomatiques, l'organisation prend la sage décision de s'associer avec des groupes militants et des médias du monde entier. En Tunisie, c'est le blog *Nawaat* qui sert de relais. WikiLeaks transmet à son équipe les documents relatifs à la Tunisie; trois de ses membres les traduisent en français et les rendent publics sous la bannière de TuniLeaks au moment où WikiLeaks diffuse les documents d'intérêt plus général. *Nawaat* s'assure aussi la collaboration de geeks et de hackers d'autres pays pour que son site web puisse rester en ligne malgré les tentatives acharnées du gouvernement de le censurer.

Les câbles diplomatiques confirment ce que tout le monde sait déjà sans en détenir la preuve: Bel Ali est pourri jusqu'à la moelle, son régime

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

est rongé par la corruption et sa famille vit dans l'opulence pendant que le reste de la population tire le diable par la queue. «La large diffusion des preuves de la corruption et de l'hypocrisie du gouvernement grâce à des fuites incessantes a joué un rôle important dans l'embrasement de la colère et l'ampleur de l'agitation chez les citoyens de la région», écrira Ibrahim Saleh, spécialiste de la politique tunisienne[5].

Beaucoup de Tunisiens lisent ces câbles où sont rigoureusement notés le nombre exact de poulets qu'on servait au tigre domestique du clan Ben Ali et les trois sortes de jus de fruit offerts à un des dîners (dont du jus de kiwi, très difficile à trouver):

> 12. (S) Le dîner comprenait une douzaine de plats, y compris du poisson, du steak, de la dinde, du poulpe, du couscous au poisson et bien plus encore. La quantité était suffisante pour un très grand nombre d'invités. Avant le dîner, une vaste sélection de petits plats ont été servis, avec trois jus de fruits au choix (y compris du jus de kiwi, qui ne sont pas facilement disponibles en Tunisie). Après le dîner, il a servi de la crème glacée et du yogourt glacé, qu'il [avait apporté] en avion de Saint-Tropez, ainsi que des bleuets, des framboises et des fruits frais et gâteau au chocolat. [...]
>
> 13. (S) Dans sa demeure, El Materi [gendre de Ben Ali] possède un tigre de grande taille («Pacha»), vivant dans une cage. Il [l'a] acquis alors qu'il n'avait que quelques semaines. Le tigre consomme quatre poulets par jour. (Commentaire: La situation a rappelé à l'ambassadeur la cage du lion d'[Oudaï] Hussein à Bagdad.) El Materi a beaucoup de domestiques. Il y en avait au moins une douzaine, dont un maître d'hôtel du Bangladesh et une nounou d'Afrique du Sud. (NB. C'est extrêmement rare en Tunisie, et très cher.)
>
> 19. (S) Cependant, le plus frappant a été l'opulence [dans] laquelle vivent El Materi et Nesrine. Leur maison à Hammamet [est] impressionnante, et avec le tigre cela ajoute à l'impression de «m'as-tu-vu». Plus extravagant: leur maison en construction à Sidi Bou Saïd, dont l'apparence serait plus celle d'un palais. Il domine les hauteurs

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> de Sidi Bou Saïd et accapare les meilleurs points de vue. Ce qui a suscité de nombreuses critiques en privé. L'opulence dans laquelle El Materi et Nesrine vivent ainsi que leur comportement explique clairement pourquoi ils, et d'autres membres de la famille de Ben Ali, sont détestés et même haïs par certains Tunisiens. Les excès de la famille Ben Ali vont crescendo[6].

La seconde allumette est craquée – littéralement – le 17 décembre 2010. Trois semaines après la divulgation des câbles diplomatiques traduits par *Nawaat*, le geste de désespoir d'un homme déchire l'âme du pays. Ce jour-là, Mohamed Bouazizi, jeune vendeur ambulant de fruits et légumes, est interpellé par la police, qui confisque sa charrette dépourvue de permis et refuse de la lui rendre malgré son intention de payer l'amende. Sa première tentative de récupérer son outil de travail est vaine; les fonctionnaires refusent même de lui parler. Humilié à deux reprises, ayant sept enfants à nourrir, il s'immole par le feu. Jusque-là impuissant et sans voix, il ne peut plus dès lors être ignoré, ce que, hélas, il a payé de sa vie.

Les premières protestations se font entendre et voir à Sidi Bouzid, la ville où habitait Bouazizi, avant de se répandre dans toutes les directions. Des manifestants sont abattus par la police, ce qui incite encore plus de gens à se joindre au mouvement. Takriz, un groupe de défense de la liberté d'expression en ligne d'abord enregistré comme liste de diffusion en 1998, tente d'intéresser la jeunesse de la rue à l'outil que constitue internet[7]. Bien qu'il n'existe aucun lien direct entre Takriz et Anonymous, les deux groupes partagent le même esprit. Réseau de quelques milliers d'internautes, Takriz refuse généralement de collaborer avec les journalistes, considère l'obscénité comme une tactique de choc et défend fièrement le principe de l'anonymat. Ce collectif de «résistants indépendants de tout le monde» diffuse ses idées «pour illuminer la Tunisie du noir total qui y règne». «Liberté, vérité et anonymat» sont ses trois piliers, et *Takrizo ergo sum* (Je Takrize, donc je suis) est sa devise[8].

Le 4 janvier 2011, Bouazizi succombe à ses brûlures. Le lendemain, une foule de 5000 personnes, selon les estimations, assiste à ses funérailles.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

«Adieu Mohamed nous te vengerons», «Ton sang n'aura pas coulé pour rien», «Nous te pleurons ce jour, nous ferons pleurer ceux qui ont causé ta perte», scandent de nombreux participants[9]. Le lendemain, 95 % des avocats du pays se mettent en grève pour dénoncer la répression[10]. Des Tunisiens de tous les milieux (enseignants, syndiqués, étudiants) se jettent dans la mêlée. Les manifestations continuent de faire tache d'huile et la violence policière, de s'intensifier. Le 13 janvier, des dizaines de journalistes, de blogueurs et de militants sont arrêtés, et plus de 60 manifestants, tués. Le 14, Ben Ali décrète l'état d'urgence, qui ne suffit pas à contenir la fureur populaire. Ce jour-là, pourtant, les grands médias occidentaux ne font pas grand effort pour rendre compte de l'ampleur des événements.

«Après tout, vous n'avez pas besoin de porter un masque pour le faire»

C'est par un bref article d'Associated Press (AP) sur les émeutes que le public nord-américain et européen apprend que la Tunisie est le théâtre d'un mouvement de contestation. Naturellement, le texte manque de détails, car la révolte vient tout juste d'éclater. Du reste, la couverture des grands médias occidentaux (à quelques exceptions près) demeurera tiède un bon moment, alors que le mouvement s'intensifie de jour en jour. Le 9 janvier (alors qu'Anonymous s'implique déjà en Tunisie comme pigeon voyageur en assurant la circulation d'enregistrements audio et vidéo recueillis sur le terrain), AP publie un autre article (repris par des quotidiens comme le *New York Times* et le *Globe and Mail*) qui, tel un perroquet, se borne à reprendre la position de Ben Ali. «Les manifestants disent dénoncer la pénurie d'emplois et d'investissements, mais les autorités indiquent que les émeutes sont attribuables à une minorité d'extrémistes qui cherchent à nuire à ce pays d'Afrique du Nord[11].» Ben Ali quittera le pays moins d'une semaine plus tard, le 15 janvier 2011.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Dans le cadre de sa campagne, Anonymous écrit une lettre aux journalistes:

> Nous avons eu vent du désintérêt de nombreux médias d'information occidentaux dignes de confiance à l'égard du soulèvement qui a cours en Tunisie. La presse libre et ouverte a la responsabilité de rapporter ce que la presse censurée est contrainte de taire. Les manifestations populaires, de même que les actions entreprises par Anonymous en solidarité avec les citoyens de Tunisie, devraient être couvertes par les grands médias.
>
> Le gouvernement tunisien, dirigé par le président Ben Ali, exerce une censure révoltante en bloquant non seulement les sites web des blogueurs dissidents, mais aussi des sites comme Flickr et toute source faisant mention de WikiLeaks. Au cours des vingt-quatre dernières heures, affichant un mépris profond pour la liberté d'expression, les autorités tunisiennes ont piraté les adresses courriel et les comptes Facebook de quiconque avait mené des actions qualifiées de «militantes» (qui peuvent être aussi «dangereuses» que l'organisation d'une manifestation et aussi innocentes qu'un commentaire sur le forum de discussion d'un groupe lié à WikiLeaks). Des comptes Facebook entiers ont été réquisitionnés par le gouvernement tunisien, dont les agents sont allés jusqu'à remplacer des photos de profil par l'image d'un navire pirate afin de se moquer des défenseurs de la liberté d'expression.
>
> À son tour, Anonymous a lancé des attaques informatiques par saturation contre les sites web du premier ministre tunisien, de son gouvernement corrompu et de la Bourse, et contre le principal serveur de noms de domaine de Tunisie, ce qui a permis le blocage de nombreux sites dont le nom se termine en .tn. De plus, nous avons fait le nécessaire pour que les Tunisiens puissent se connecter à internet de façon anonyme et avoir accès à des informations que leur gouvernement souhaite leur cacher.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Ces événements n'ont pas fait l'objet d'une couverture digne de ce nom. Nous vous posons la question suivante: pourquoi une source d'informations comme Al Jazeera est-elle presque seule à rapporter ce soulèvement d'envergure? Le monde commence à avoir l'impression que nos médias ne daignent couvrir un événement que si des intérêts économiques occidentaux sont en jeu.

Mais peut-être n'étiez-vous pas au courant? Maintenant que vous l'êtes, aidez-nous à diffuser la nouvelle. Après tout, vous n'avez même pas besoin de porter un masque pour le faire.

Cordialement,

Anonymous[12]

«Croyez-moi, le truc, c'est de ne pas avoir d'égo»

Mais Anonymous ne se contente pas d'exhorter les grands médias à faire leur travail. Le 2 janvier 2011, une équipe technique réunie sur #internetfeds renonce à ses vacances pour travailler sans relâche. Adnon me racontera d'ailleurs n'avoir presque pas dormi pendant deux semaines. Les Anons adoptent une stratégie différente de celle des opérations Payback et Avenge Assange:

<Adnon> Pour la Tunisie, on avait un plan
<Adnon> On avait soigneusement réfléchi en petit groupe à ce qu'on allait faire et au moment où on le ferait
<Adnon> on avait soumis une liste de possibilités à la consultation
<Adnon> puis recueilli les résultats de la consultation
<Adnon> Les décisions ont été prises par un groupe beaucoup moins grand que lors des autres opérations

L'opération Tunisie a marqué un changement radical tant au sein du collectif que dans la façon dont il était perçu par le grand public. Pendant tout l'automne, Anonymous avait été au confluent d'une multitude de cabales et de canaux secrets. Même Chanology avait dû tenir compte de

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

marblecake, une faction issue de ses propres rangs. Si les membres de ces canaux secrets détenaient une autorité technique et, à maints égards, menaient le bal, ils avaient besoin de leurs camarades des canaux publics pour faire bouger les choses. Les citoyens d'IRC en colère avaient su modérer leurs ardeurs, comme l'avait si bien démontré le soulèvement massif du début de l'automne contre la décision de #command d'acquiescer à la demande du Parti pirate, qui réclamait la fin des attaques par saturation.

Mais l'opération Tunisie a été gérée autrement: dès le départ, une poignée de petites équipes composées de hackers, de propagandistes et d'organisateurs ont pris les commandes, qu'ils n'abandonneraient pas. La prééminence de ce réseau d'équipes n'excluait toutefois pas des modes d'organisation de masse. D'autres opérations se déroulaient simultanément, dont certaines émanaient de canaux publics. Un canal public voué à l'opération Tunisie a d'ailleurs joué un rôle important.

Le 2 janvier 2011, un hacker appelé rubik (pseudo modifié), actif sur deux canaux privés, annonce qu'un site web tunisien vient d'être défacé (tous les pseudos ont été modifiés):

> <rubik> http://www.pm.gov.tn/pm/index.php — défacé
> <OT> Excellent, Anons!!!
> <OT> Bravo!
> <rubik> C'est clair! Beau travail!
> <OT> Il en reste, les copains:P
> <rubik> aussi http://www.marchespublics.gov.tn
> <K-rad> http://www.pm.gov.tn et
> http://www.marchespublics.gov.tn/ — DÉFACÉS!
> <lafdie> en passant, un gros merci pour les lolcats:
> http://www.pm.gov.tn/pm/index.php
> <vvom> http://www.pm.gov.tn/pm/index.php HOURRA POUR LES SALOPARDS

On avait là des hackers qui travaillaient d'arrache-pied, en équipe, depuis un certain temps, et, pourtant, les journalistes n'ont pu résister à la tentation de désigner un «cerveau», un «chef», un architecte qui aurait manipulé tous

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

les autres. Chose ironique, en recherchant «*Anonymous leader*» sur internet, on obtient au moins quatre noms différents. Les journalistes ont fini par désigner Sabu et Topiary, sans doute parce qu'ils confondaient la présence publique plus forte de ces Anons avec quelque contrôle organisationnel (ou dictatorial) de leur part[13].

Si de nombreux articles mentionnaient un «meneur» ou un «cerveau», ce que le choix d'un tel angle voulait précisément dire restait implicite. Le lecteur pouvait donc laisser aller son imagination, par exemple se figurer un grand méchant en costume trois-pièces, confortablement installé dans un profond fauteuil, en train de caresser son chat persan pendant que son rire diabolique résonne dans les vastes salles d'un palais de glace. En se basant sur les journaux d'un serveur IRC ayant fait l'objet d'une fuite, le journaliste Adrian Chen, par exemple, a avancé que «Sabu joue le rôle d'un chef qui fait respecter la discipline pendant que les autres membres sont prêts à agir[14]». Ce qui ne l'a pas empêché de se contredire juste après, alors qu'il parlait d'une opération de hacking connexe menée indépendamment de Sabu par un autre groupe d'Anons. C'est qu'analyser une seule entrée de journal* (*log*) pour démontrer la présence d'un chef est à peu près aussi efficace que d'extrapoler l'ensemble du scénario d'un film à partir d'un arrêt sur image. Charles Arthur a fait la même erreur dans *The Guardian*: «Dans la période qui a suivi les arrestations au Royaume-Uni, le seul membre visiblement actif de LulzSec était son chef, connu en ligne sous le pseudo de Sabu, qui, simultanément, niait en être le chef et utilisait des expressions comme "mon équipe"[15].» Le contexte permet cependant de constater que Sabu parlait tout simplement du canal #pure-elite, qu'il avait créé il y a longtemps, et que d'autres membres de LulzSec qualifiaient d'«endroit où glander avec ses potes».

En fait, les opérations de hacking, en particulier celles d'Anonymous, sont généralement dynamiques et fluides; elles sont le fait d'une multitude d'individus – voire de groupes – qui travaillent de concert. Chacune d'elles peut avoir ses propres caractéristiques. Dans un cas, un hacker particulièrement déterminé aura réparti le travail collectif avec rigueur; dans un autre, l'action se produira dans le désordre et la cacophonie. D'ailleurs,

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

quand j'ai interviewé Jeremy Hammond en prison beaucoup plus tard, il a déploré cette inconstance: «J'aimerais que nous ressemblions un peu plus à RedHack, que nous soyons plus disciplinés.» Groupe de hackers militants basé en Turquie, RedHack se caractérise par sa hiérarchie claire, avec chef et porte-parole, fruit de seize ans d'organisation et de fidélité aux principes du marxisme-léninisme.

Peut-être les exploits d'Anonymous auraient-ils été plus remarquables si le groupe avait eu un chef ou une hiérarchie rigide. Les hackers ont tendance à être affligés de ce que je me plais à appeler le «trouble de la distraction du geek». Livré à lui-même, un hacker peut facilement aboutir dans un champ, entouré de yacks, avec un rasoir à la main, à se demander comment il a bien pu se retrouver là (si cette allusion vous dit quelque chose, vous êtes concerné!). Mais il est également probable qu'Anonymous affiche un bilan aussi impressionnant précisément parce qu'aucun chef ne lui a imprimé d'orientation déterminée. Quoi qu'il en soit, les efforts du collectif se sont déployés de manière organique, c'est-à-dire en fonction des gens qui fréquentaient un canal, de leur contribution singulière et de leur volonté d'apprendre quelque chose de nouveau, ingrédient essentiel à toute entreprise de hacking fructueuse.

L'opération Tunisie illustre parfaitement cette dynamique. Imaginez-vous en Anon constatant le déclenchement de l'opération sur IRC. En ce 2 janvier 2011, vous êtes en contact direct avec des militants et des hackers tunisiens qui vous transmettent des informations brutes sur une révolte d'importance historique. Vous êtes chez vous, assis, complètement immobile à l'exception de vos doigts qui parcourent le clavier, mais les données que vous recevez vous permettent de modifier directement le cours des événements, presque autant que le font les insurgés qui, sur le terrain, lancent des cocktails Molotov. Votre contribution est peut-être modeste, mais elle compte. Elle est valorisante sur le plan personnel, elle constitue un geste de solidarité et représente sans doute un atout précieux pour certains insurgés, à la protection desquels elle contribue. Tout cela repose sur des modes de coopération changeants et désordonnés – et crée un climat permettant à des organisations de prendre leur essor en saisissant une bonne

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

idée au vol, puis de s'effondrer au moindre signe de désaccord sur la voie à emprunter.

À ce stade-ci des opérations, deux canaux IRC privés sont actifs simultanément: #opdeface et #internetfeds. Le premier est un espace où les organisateurs se rassemblent, tandis que le second est consacré aux tâches techniques les plus fastidieuses. Un messager fait circuler les informations entre les deux. Certains hackers sont au courant, tandis que d'autres sont de nouveaux venus (tous les pseudos ont été modifiés):

> <rubik> K-rad, tu sais te servir de PostgreSQL? [PostgreSQL est un système de gestion de base de données]
> <rubik> http://www.pm.gov.tn/pm/banniere/redirectb.php?id=54&idb=3'2&
> <K-rad> rubik, j'ai jamais eu affaire à PostgreSQL, c'est même la première fois que je le vois, franchement
> <gibnut> pourquoi on attaque la tunisie?
> <K-rad> Parce qu'ils viennent d'adopter une loi qui interdit aux médias de dire ce qu'ils veulent
> <K-rad> et de mentionner wikileaks
> <gibnut> K-rad, merci!
> <gibnut> il est temps de prendre le contrôle de la tunisie, alors;)

Sur d'autres canaux, certains participants proposent de mener des campagnes d'attaques par saturation, mais, tant chez Anonymous qu'ailleurs se trouvent des gens qui se targuent d'être de «vrais» hackers et rejettent cette stratégie, jugée inefficace, voire nuisible aux véritables opérations de hacking, comme nous le verrons plus loin. Les vrais hackers sont en quête d'*exploits**. Selon eux, les gens qui se contentent de se servir de Low Orbit Ion Cannon (LOIC) ne méritent pas le titre de hacker et ne sont que de vulgaires *skiddies*. gibnut annonce alors qu'il vient de découvrir une vulnérabilité jour zéro, un type de faille qui permet de causer des dommages nettement plus importants. Calque de l'anglais *zero-day*, ce terme désigne une vulnérabilité jusque-là inconnue d'un logiciel ou d'un système informatique. On l'appelle «jour zéro» parce qu'elle est inconnue

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

du public (ou des programmeurs du logiciel en cause, qui pourraient lui apporter un correctif) à zéro jour de la sortie du programme. Une vulnérabilité jour zéro vaut de l'or; quiconque en connaît l'existence peut en tirer parti jusqu'à ce qu'un correctif y soit apporté. Les plus convoitées de ces vulnérabilités permettent d'avoir accès à un ordinateur ou à un réseau, ce qui explique pourquoi elles se vendent très cher sur un marché noir en plein essor. De nombreux gouvernements participent à ce marché à l'éthique douteuse, dont celui des États-Unis, qui, selon le journaliste techno Joseph Menn, «est devenu le plus gros acheteur sur un marché gris où des hackers et des firmes de sécurité informatique vendent des outils permettant de s'introduire dans des ordinateurs[16]». Les États-Unis achètent la plupart de leurs vulnérabilités jour zéro de sociétés privées qui «investissent au bas mot des dizaines de millions de dollars par an dans les seuls *exploits*[17]». Il va sans dire que l'annonce de gibnut est accueillie avec enthousiasme:

> <gibnut> oublions loic, attaquons-les autrement
> <p-ground> oh oui svp
> <gibnut> j'ai un exploit contre une vulnérabilité jour zéro d'openwebmail, utilisé par les serveurs du registraire de noms de domaine tunisiens
> <gibnut> https://risala.ati.tn/cgi-bin/openwebmail/openwebmail.pl
> <gibnut> si on parvient à entrer dans ce serveur, on sera à la racine des serveurs de nom de domaine de premier niveau .tn et on contrôlera tout l'espace internet de la tunisie
> <p-ground> putain
> <gibnut> redirigeons le tout à wikileaks
> <p-ground> la merde prend forme grâce à gibnut

Muni de cette vulnérabilité jour zéro, gibnut affirme que les Anons sont en mesure de nuire au registraire de noms de domaine tunisiens et de contrôler l'ensemble du domaine de premier niveau du pays. (Le domaine de premier niveau est représenté par le dernier élément d'un nom de domaine, comme

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

«.com» ou «.org». Chaque pays dispose de son propre domaine de premier niveau; celui de la Tunisie est «.tn».) Si les Anons parviennent à compromettre ce registraire, ils pourront réacheminer toute requête pour un site web dont le nom se termine en «.tn» vers le serveur de leur choix. Dans l'esprit du *lulz*, gibnut propose WikiLeaks. Toutefois, pour des raisons inconnues, l'attaque ne se concrétisera pas. Le projet aboutit cependant par la bande en répandant un optimisme fougueux[18]:

> <gibnut> laissez-moi voir si je peux faire quelque chose... je reviens tout de suite
> <p-ground> Armez les têtes nucléaires, les gars
> <p-ground> Internetfeds arrive
> <K-rad> gibnut,:D très bien <3
> <K-rad> mais il faut d'abord trouver un bug là-bas
> <jaggy91> épique
> <p-ground> pour une raison quelconque, tout ce qui se passe sur ce canal finit par être épique
> <jaggy91> lol
> <rubik> j'imagine que j'aurai besoin d'un aide-mémoire pour l'injection de code sur PostgreSQL ou un truc du genre
> <gibnut> rubik, ou télécharge havij pour windows
> <K-rad> http://www.marchespublics.gov.tn est HAUTEMENT INJECTABLE:3 [il comporte au moins une vulnérabilité qui permet à un attaquant de modifier la base de données du site autrement que prévu]
> <K-rad> on est prêts pour le lulz <3
> <rubik>:o
> <rubik> ça ressemble au ministère de la justice, je crois, je sais pas
> <K-rad> je sais pas, mais UNE GRANDE PARTIE de ces sites sont vulnérables

S'il constate qu'il ignore quelque chose, tout bon hacker entreprend de s'instruire:

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> <K-rad> connaissez ce bug de postgresql?
> <rubik> ouais
> <K-rad> j'ai lu qq trucs sur postgresql et j'en ai appris sur les bases de données, alors je sais maintenant comment faire l'injection:D
> <K-rad> tenez-vous prêt à sauvegarder la BD

K-rad disparaît un bon moment, pendant lequel il travaille sûrement dur, puis revient avec des résultats. Il a eu accès à une base de données de 1 600 entrées et a tenté d'en craquer les mots de passe. Il commence par s'excuser («dsl les gars, ça m'a pris du temps parce que j'avais jamais travaillé sur PostgreSQL et que j'essaie d'écrire un script pour aller plus vite»), puis il réalise que la lenteur de l'obtention des mots de passe est due à une attaque par saturation en cours. Il implore ses camarades:

> <K-rad> que quelqu'un dise à optunisie de ne pas attaquer 193.95.68.156, ça bousille ma sauvegarde

Pendant ce temps, comme il s'agit d'un effort collectif, d'autres hackers recherchent aussi des vulnérabilités informatiques qui leur ouvriraient les portes des serveurs tunisiens. S'ils avaient accès à l'interface système, ils pourraient mettre la main sur les courriels personnels du premier ministre tunisien, puis les divulguer. rubik y parvient. Il ne trouve malheureusement que des pourriels, mais ce revers ne met pas fin à la tentative d'«appropriation» visant à rendre accessible la racine du système, ce qui permettrait à ces Anons d'y intervenir à leur guise: ils pourraient y lire et y modifier tous les fichiers, intervenir sur les processus en cours, y implanter leurs propres processus et codes malicieux, ou encore, si tel était ce qu'ils souhaitent, tout effacer. Ils deviendraient ainsi les administrateurs de la machine, même s'ils se trouvent à des milliers de kilomètres. Sans surprise, ils défaceront le site, mais pas avant d'avoir tenté de récupérer des courriels:

> <rubik> je me suis connecté, mais y a rien

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<K-rad> je reviens les gars, je vais me faire un p'tit thé:3
<gibnut> http://www.marchespublics.gov.tn/onmp/upload/upload_fichier.php?Field=document&type=document
<gibnut>;]
<gibnut> je me l'approprie maintenant ou plus tard
<rubik> super
<K-rad> mieux vaut y aller tout de suite pendant que la vapeur anti-tuni.gov monte encore
<rubik> on pourrait télécharger une interface système, j'imagine
<gibnut> tellement
<rubik> quelle interface aimeriez-vous les gars;]
<rubik> j'en ai genre 40
<K-rad> ça boostera l'effet et le moral des troupes
<K-rad> si on a accès à la racine, on pourrait aussi balancer les courriels
<K-rad> et pas seulement défacer
<K-rad>:D
<K-rad> une mégafuite de courriels:D:D
<rubik> j'ai trouvé l'interface système
<gibnut> www.marchespublics.gov.tn/onmp/upload/documents
<K-rad> que quelqu'un crée une jolie page de défaçage svp:3

Alors que l'équipe s'apprête à défacer la page, K-rad déclare avec enthousiasme que le noyau du système d'exploitation du serveur est désuet. Le noyau est l'élément central d'un système d'exploitation, l'interface entre les composants logiciels et matériels d'un ordinateur. La présence d'un vieux noyau indique que le système a fait l'objet d'*exploits* répertoriés, ce qui est presque toujours bon signe pour une personne qui envisage de compromettre une machine:

<rubik> voici une page pour le défaçage
<rubik> http://pickhost.eu/images/0004/1986/anonymousdefacetunisia.j

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

pg
<rubik> si elle vous plaît
<rubik>:p
<K-rad> VIEUUUUUUUUUUUUUUUX NOYAU, À NOUS LA VICTOIRE
<rubik> racine?
<duckie> pas mal rubik
<duckie> mais tu pourrais pas centrer le texte du bas?
<rubik> je sais pas, je l'ai pas fait
<rubik> je travaille sur tor
<rubik> j'aimerais avoir un vpn

duckie vient de se connecter au canal pour donner un coup de main. Ses compétences limitées en hacking des profondeurs lui vaudront plus tard d'en être chassé, mais il est très doué comme organisateur et comme négociateur, si bien qu'on lui permet pour le moment de fréquenter #internetfeds. Il possède un talent rare pour trouver des noms aux opérations et observe les changements qui touchent AnonOps avec une perspicacité remarquable:

<duckie> Y a-t-il quelque chose que je peux faire qui ne demande pas de s'introduire dans le serveur?
<duckie> rubik, je suis pas venu souvent, ce canal était censé être mort depuis longtemps
<K-rad> duckie, fais une page de défaçage!:D?

Alors que #internetfeds cherche fébrilement les courriels privés du premier ministre de Tunisie, un autre canal, #opdeface, déborde aussi d'activité. Cependant, même dans le canal d'élite qu'est #internetfeds, nombreux sont les participants qui ignorent l'existence de #opdeface. La recherche de courriels s'avère vaine. Sur #opdeface, rubik rapporte l'*exploit* déniché sur #internetfeds.

Des Anons tunisiens réalisent alors qu'un *exploit* pourrait fonctionner avec une autre cible:

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<OT> Je répète: la cible principale est l'ati [agence tunisienne d'internet]
<OT> Directement responsable de la censure
<mo> j'ai trouvé une faille XSS à exploiter sur le site de l'ati
<a> OT, lol, j'ai cru que t'avais dit ça sur un canal public
<OT> lol
<OT> suis pas encore si défoncé...
<rubik> on a trouvé des mots de passe d'administrateurs pour marchespublics.gov.tn, qui est actuellement dans la même boîte que pm.gov.tn
<vj> si je me souviens bien, on avait prévu une attaque par saturation contre le ministère de la communication
<vj> si elle a été annulée, je sais pas pourquoi
<a> ce n'était qu'une possibilité parmi d'autres

Croyant pouvoir mettre la main sur des courriels juteux, rubik leur demande de l'aide:

<rubik> en passant
<rubik> est-ce que quelqu'un pourrait rédiger une déclaration
<rubik> pour décrire le torrent
<rubik> quand on obtiendra les courriels de pm.gov.tn
<rubik> c'est-à-dire un message annonçant à pm.gov.tn que leurs courriels ont été fuités
<rubik> mais pas tout de suite
<rubik> faites d'abord une page de défaçage
<rubik> à moins que http://pickhost.eu/images/0004/1986/anonymousdefacetunisia.jpg vous convienne
<rubik> puis préparez une description du torrent ou un manifeste

Des membres de #opdeface finissent par rédiger une déclaration:

<vj> Salutations de la part d'Anonymous.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<vj> Nous avons observé le traitement que vous réservez à votre propre population, et nous sommes à la fois extrêmement attristés et irrités par votre comportement. Vous avez unilatéralement déclaré la guerre à la liberté d'expression, à la démocratie et même à votre propre peuple. Si votre population manifeste dans les rues, c'est parce qu'elle exige que vous lui rendiez des comptes et que vous respectiez ses droits, que vous avez cru, à tort, avoir la prérogative de lui retirer.
<vj> Nous profitons de ce bref moment où nous avons capté votre attention pour vous livrer un message clair, actuel, qui, nous l'espérons, ne sera jamais oublié. Souvenez-vous bien de ceci: plus vous écraserez votre population, plus elle contestera votre autorité. Plus vous la serrerez fort au creux de votre poing, plus elle s'en écoulera comme une poignée de sable. Plus vous la censurerez,
<vj> plus elle en saura sur vous et sur ce que vous faites.
<vj> Nous sommes Anonymous.
<vj> Nous sommes l'incarnation de la liberté d'expression en colère.
<vj> Nous sommes le système immunitaire de la démocratie.
<vj> Nous ne pardonnons pas la censure.
<vj> Nous ne laissons pas tomber la liberté d'expression.
<vj> Attendez-vous à notre présence, toujours.
<a> c'est bon. je remplacerais population par citoyens
<a> ça sonne plus... profond
<vj> Nous profitons de ce bref moment où nous avons capté votre attention pour vous livrer un message clair, actuel, qui, nous l'espérons, ne sera jamais oublié. Souvenez-vous bien de ceci: plus vous écraserez vos citoyens, plus ils contesteront votre autorité. Plus vous la serrerez fort au creux de votre poing, plus elle s'en écoulera comme une poignée de sable. Plus vous les censurerez,
<vj> plus ils en sauront sur vous et sur ce que vous faites.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> <vj> Dans cet esprit, nous diffusons auprès des citoyens tunisiens et du monde entier un cache de documents gouvernementaux. Nous espérons ainsi faire la lumière sur ce que le gouvernement tente désespérément de cacher.

rubik continue de faire le messager entre les deux canaux. Une fois cette étape de la campagne franchie, il en attribue le mérite à l'un des membres de l'équipe – lequel, soit dit en passant, n'est pas Sabu, mais K-rad. Au nom de l'éthique, un autre Anon s'empresse de condamner cet éloge d'un seul individu, et K-rad lui-même atténue la valeur de sa prouesse – une illustration parfaite de la modestie valorisée chez les Anons:

> <rubik> le mérite de celle-là revient à K-rad
> <K-rad> à tous les membres de feds:D
> <K-rad> n'oubliez pas de rm –rf* leur page d'ouverture de session d'administrateur [rm –rf est la commande permettant d'effacer un répertoire]
> <K-rad> et de rm –rf tout ce que vous pouvez avec ces permissions
> <Adnon> Vous l'avez fait, les gars
> <a> n'oublions pas gibnut
> <a> et tous ceux qui ont travaillé dans l'ombre (=
> <OT> pas de noms lol seulement des anonymes
> <a> euh, bien sûr
> <a> mais ici, les gens qui sont ici...
> <nessy> nous agissons en secret, cependant
> <a> ça tient toujours, j'imagine (=
> <OT> croyez-moi, les mecs, ne pas avoir d'égo est indispensable à nos projets
> <a> nous ne faisions que nous féliciter
> <a> en interne:)
> <OT> lol
> <alex> eh
> <alex> bien sûr

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<gibnut> pas de noms svp:)

Alors voilà à quoi ressemblent des hackers à l'œuvre. Du travail d'équipe certes typique, mais tout de même impressionnant et plutôt drôle, du moins pour les personnes qui l'effectuent. J'ai cité deux canaux seulement, mais la campagne a été menée par au moins quatre groupes distincts, sans parler du bloc-notes collaboratif destiné à la rédaction des communiqués de presse. Il faut aussi garder à l'esprit que le canal public #propaganda (mobilisé pour l'opération Tunisie) et le canal privé #command étaient actifs au même moment, et que de nombreux Anons se coordonnaient également par messagerie privée.

En résumé, Anonymous possède tellement de tentacules que l'idée même d'un chef qui tiendrait les leviers de commande est absurde: le collectif n'est ni une ruche (comme il se définit souvent lui-même), ni une masse informe, ni une hiérarchie bien structurée, mais un peu de tout cela à la fois.

«Ne vous en faites pas, moi aussi, je suis anonyme»

Comme nous venons de le voir, dans toute situation, il arrive que certaines personnes se démarquent par leurs aptitudes – ce fut manifestement le cas de K-rad dans le cadre de l'opération Tunisie. Au fil du temps, cependant, les contributions de chacun déteignent les unes sur les autres et l'individu finit par se diluer. Pourtant, tout en gardant cela à l'esprit, il peut être instructif de renverser le point de vue, soit d'isoler, au sein d'Anonymous, un participant et ses opérations. Cela permettra de réfuter une autre fausse conception qui colle à la peau du collectif. En effet, en soulignant la contribution de tflow à l'opération Tunisie et en la mettant en parallèle avec celles d'Adnon et d'Amamou, on constate que l'image qu'on se fait de l'Anon typique (un homme blanc, de la classe moyenne, libertarien et politiquement naïf) est très éloignée de la réalité.

Programmeur talentueux, tflow (présenté ci-dessus sous un autre pseudo) est devenu membre d'Anonymous à l'automne 2010 et a fondé

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

#internetfeds, l'aile secrète du collectif vouée au hacking. Pendant une bonne partie de la saison, il en a été le «maître des clés», chargé de soumettre trois questions techniques aux potentielles recrues afin d'évaluer leurs compétences en hacking. Pendant l'opération Tunisie, ce technicien parmi les plus prolifiques d'AnonOps a eu l'idée astucieuse d'écrire un script antihameçonnage. En gros, la notion d'hameçonnage désigne toute méthode employée pour récupérer des données privées (en général des combinaisons de noms d'utilisateurs et de mots de passe ainsi que des numéros de carte de crédit) en prétendant être une personne ou une organisation digne de confiance. Une des techniques courantes consiste à envoyer à la personne visée des courriels falsifiés qui semblent provenir du centre d'assistance de son service de messagerie (ou encore de son institution bancaire), courriels qui lui demandent d'indiquer son nom d'utilisateur et son mot de passe sous peine de fermeture du compte. Une variante plus sophistiquée du message contient un lien qui, lorsqu'ouvert, provoque l'installation d'un enregistreur de frappes ou autre logiciel malveillant sur l'appareil de la victime. Un taux alarmant de ces attaques atteignent leur but, ce qui en fait un stratagème très lucratif. «Des expériences ont démontré que l'hameçonnage enregistre un taux de réussite de 70 % dans les médias sociaux», a conclu une étude menée par des informaticiens[19]. Par conséquent, il n'est guère surprenant que le régime de Ben Ali se soit livré lui-même à cette tactique pour mettre la main sur les noms d'utilisateur et mots de passe des comptes de médias sociaux de militants tunisiens. L'idée de tflow consistait à trouver un antidote efficace à ce script, lequel prendrait également la forme d'un script.

Le script de tflow était l'exemple parfait du «hacking ingénieux», auquel Jude Milhon, plus connue sous son pseudo St. Jude, a donné cette élégante définition: «Le hacking est un contournement astucieux des limites imposées par un gouvernement, par un serveur internet ou par la propre personnalité du hacker[20].» Le script en question n'était pas très sophistiqué; tflow en avait écrit le code en moins de dix minutes, et il aurait pu le faire en trente secondes s'il en avait mieux maîtrisé la technologie

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

sous-jacente. Si ce script peut être qualifié d'outil de hacking ingénieux, c'est tout simplement parce qu'il répondait à un besoin et qu'il fonctionnait.

Pour être en mesure de préparer son petit programme, tflow devait d'abord se procurer le script malveillant. Pour ce faire, il lui fallait trouver un Tunisien disposé à le laisser contrôler son ordinateur à distance à l'aide d'un logiciel appelé TeamViewer. Début janvier 2011, il est donc entré en contact avec un militant tunisien (tous les pseudos sont modifiés sauf celui de tflow):

> <tflow> anont
> <anont> oui, tflow
> <tflow> anont, es-tu en tunisie?
> <anont> oui, tflow
> <tflow> peux-tu aller sur teamviewer pour qu'on puisse trouver l'adresse ip reliée aux scripts d'hameçonnage et les hacker?

Bien sûr, anont a posé la question incontournable:

> <anont> tflow, qu'est-ce qui me dit que je peux te faire confiance?
> <shaka> tflow est tout à fait digne de confiance
> <oggle> tflow est un membre fiable
> <Aa> anont, je crois que plusieurs personnes pourraient répondre de tflow, et j'en fais partie

Parce que la confiance n'est souvent qu'affaire de foi, tflow a lui-même donné l'avis le plus pertinent (et quelqu'un a fait une «blague» de mauvais goût):

> <tflow> anont, tu peux voir tout ce que je fais sur ton écran; si tu n'aimes pas ça, tu peux arrêter
> <shaka> tflow est de la vielle école, il a été de l'opération payback
> <k02> faites confiance à tflow: il vous file toujours des bonbons après vous avoir violé!

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

anont a répondu:

<anont> Aa, tflow, shaka, OK. contacte-moi en privé

tflow pouvait maintenant écrire son script. Assez simple, celui-ci devait avoir pour effet de modifier les fonctions du script gouvernemental en vue de les rendre inopérantes. Le lendemain, alors que le petit programme, mis en ligne, était en cours de téléchargement par des milliers de personnes, tflow et anont ont eu une nouvelle conversation privée:

<tflow> salut
<tflow> toujours là?
<anont> oui
<tflow> lance teamviewer
<tflow> je veux voir si le script fonctionne
<anont> bon travail! bravo
<anont>:) [...]
<anont> salut
<anont> j'ai des nouvelles
<tflow> salut
<anont> le journaliste d'aljazeera va enquêter sur l'hameçonnage via fb, google et cie
<tflow> super
<tflow> il y a aussi un article sur le sujet ici http://www.thetechherald.com/article.php/201101/6651/Tunisian-governmentharvesting-usernames-and-passwords, c'est bien expliqué
<anont> oui
<anont> je l'ai transféré à plusieurs médias hier soir
<tflow> super
<anont> je suis moi-même journaliste
<tflow> est-ce que tu leur as aussi envoyé le script antihameçonnage?
<tflow> ah

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<anont> oui
<anont> t'en fais pas
<anont> je suis anonyme moi aussi:D

Effectivement journaliste, anont a gardé l'anonymat, mais j'ai eu la chance de rencontrer tflow en personne à Londres, en juillet 2013, soit deux ans presque jour pour jour après son arrestation par la police du Grand Londres. Le hacker, mis en accusation pour utilisation malveillante d'un ordinateur, a plaidé coupable et a admis avoir conspiré en vue de hacker les serveurs de nombreuses organisations britanniques ou internationales, dont la Serious Organised Crime Agency, 20th Century Fox et News International. Mineur au moment des faits, il s'en est tiré avec une sentence clémente de travaux d'intérêt collectif. Les travaux en question ont consisté «à poser des étiquettes de prix sur des vêtements donnés, à les disposer en magasin et à revoir la conception des vitrines», m'a-t-il dit lors d'une interview.

Je n'ai pas passé beaucoup de temps à discuter avec tflow, et surtout pas en privé. Son nom apparaissait constamment sur mon écran et, à l'occasion, nous chattions, généralement dans le cadre d'une conversation de groupe. Très éloquent et plein d'esprit, ses conversations étaient toujours un mélange de technique et de philosophie. Il était parfois trop sûr de lui, mais sans arrogance, et cela menait souvent à élargir le point de vue. Prenons l'exemple de cette conversation de mars 2011, ayant eu lieu sur un canal IRC pour journalistes, #reporter. Une journaliste qui venait de se connecter pour la première fois demandait:

<reporter799> comment ça marche?
<reporter799> je suis nouvelle
<tflow> magie
<tflow> sorcellerie
<reporter799> haha
<reporter799> alors, quand vous donnez des interviews, comment on fait exactement?
<Token> Posez une question, quelqu'un répondra
<reporter799> je veux dire, en général, sur ce forum?

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<tflow> eh bien, les lois de la physique déclencheront des réactions chimiques dans votre cerveau pour qu'il formule une question, feront bouger les muscles de vos bras pour qu'ils donnent forme à votre question, puis, quand vous appuierez sur la touche enter, celle-ci sera transmise par les tubes
<tflow> ouais, n'avez qu'à poser votre question ici
<Token> lol tflow
<reporter799> et attribuer la citation à un «membre du groupe Anonymous»?
<tflow> la plupart des gens qui fréquentent ce canal ont pris part à des opérations d'Anonymous
<reporter799> c'est encourageant [...]
<tflow> pour quelle publication/chaîne d'information travaillez-vous?
<reporter799> pigiste
<reporter799> j'écris pour [X] et j'ai mon propre blog
<reporter799> je vous enverrai un lien [elle l'envoie]
<tflow> parfait
<reporter799> Bon, j'imagine que je peux commencer à poser des questions?
<tflow> je ne vois pas très bien le rapport entre un blog sur les rencontres amoureuses et ce qui nous occupe ici, néanmoins:P

tflow fréquentait régulièrement les canaux IRC, mais sa localisation géographique était difficile à déterminer. Il était manifestement de langue maternelle anglaise, mais cette information n'était pas d'un grand secours pour circonscrire son lieu de résidence. Jamais la possibilité d'avoir affaire à un adolescent, comme Adnon, ne m'avait traversé l'esprit. Le 19 juillet 2011, lorsqu'il s'est fait arrêter et a révélé être âgé de 16 ans, la stupéfaction a retenti jusque dans les rangs d'AnonOps. Tout le monde était surpris: le travail d'équipe n'avait pas empêché ses collègues hackers de reconnaître son savoir-faire et ils le considéraient comme le plus brillant d'entre eux.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Parce qu'il était mineur au moment de son arrestation, les autorités n'ont pas divulgué son identité. J'ai un peu honte de l'admettre, mais, quand j'ai appris qu'il était britannique et adolescent, une image m'est immédiatement venue à l'esprit. Elle n'était pas aussi fausse que celle de ces «nihilistes, anarchistes, militants et membres de LulzSec ou d'Anonymous dans la vingtaine qui n'ont pas parlé à une personne du sexe opposé depuis cinq ou six ans», brossée par Michael Hayden, ex-directeur de la Central Intelligence Agency (CIA) et de la National Security Agency (NSA) pour décrire les sympathisants d'Edward Snowden[21]. Je visualisais plutôt un enfant abandonné au teint blême, placé en pensionnat dès son plus jeune âge par ses parents, riches et négligents.

Finalement, quand il a eu 18 ans, on a su que tflow était en fait Mustafa Al-Bassam, et ses photos ont confirmé qu'il était loin d'être pâlichon. Ayant fui l'Irak de Saddam Hussein, ses parents s'étaient installés à Londres avec lui alors qu'il avait six ans. Son père est médecin généraliste, sa famille appartient donc à la classe moyenne supérieure. Elle habitait cependant à l'époque un quartier pauvre du sud de Londres, peuplé d'immigrants, et son train de vie était plutôt proche de celui de la classe ouvrière. À l'instar de nombreux immigrants, ses parents étaient plus portés sur l'épargne que sur la dépense. Quand je l'ai pressé de questions sur ses origines, il m'a répondu avec un certain inconfort: «Nous vivons dans une des zones les plus économiquement et socialement défavorisées du Royaume-Uni.» Notre première rencontre londonienne s'est avérée tendue et embarrassée (contrairement à mon entretien avec Adnon), car nous n'avions pas passé des centaines d'heures à faire connaissance en ligne. Cette impression de distance était sans doute amplifiée par le fait qu'il était sorti du milieu depuis un certain temps, car le juge lui avait interdit de se connecter à internet pendant deux ans. Heureusement, le soleil qu'il faisait ce jour-là (le Royaume-Uni profitait d'une rare éclaircie) a contribué à adoucir l'atmosphère.

Nous avons poursuivi notre conversation en ligne. Un de nos sujets de discussion récurrents était la moralité de la loi, ce qui n'était guère surprenant vu l'expérience personnelle d'Al-Bassam avec le système

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

judiciaire. Un jour, nous avons parlé d'un autre jeune hacker, Aaron Swartz, piégé par la justice américaine. (Swartz était un des fondateurs du populaire site de partage de liens Reddit.) À l'âge de 25 ans, il risquait d'être condamné à trente-cinq ans de prison et à un million de dollars d'amende pour avoir téléchargé des articles scientifiques de la base de données savante JSTOR, accessible à tout membre du réseau du Massachusetts Institute of Technology (MIT).

S'il avait été reconnu coupable, il n'aurait sans doute pas été condamné à une si lourde peine. Mais la poursuite a invoqué le nombre de chefs d'accusation et la durée potentielle de l'emprisonnement qu'il pourrait encourir pour le pousser à reconnaître son crime et à négocier sa peine. Le plus étonnant, c'est qu'il n'avait nullement «hacké» le site de JSTOR, et que l'éditeur du site en question n'avait engagé aucune poursuite contre lui. Certes, l'affaire avait occasionné des frais au MIT, mais sans nuire bien sérieusement. Le principal procureur du département de la Justice dans cette affaire, Stephen Heymann, a eu néanmoins l'outrecuidance de comparer «ce pionnier d'internet à un violeur, et d'affirmer qu'il s'était "systématiquement acharné" contre le MIT en refusant la négociation de peine», écrivit Ryan Reilly dans le *Huffington Post*[22].

Sans doute aurait-il pu être jugé coupable d'intrusion (il avait planqué un ordinateur dans un placard du campus et l'avait branché directement au réseau du MIT). À quelques reprises, les administrateurs du réseau l'avaient banni, sans doute dans le but de l'empêcher de télécharger plus d'un certain nombre d'articles. Cependant, même si ses gestes étaient illégaux ou contrevenaient aux règlements, on pourrait, au nom de principes moraux, soutenir que le téléchargement d'articles scientifiques (fruits de recherches financées en grande partie par des fonds publics) ne mérite pas d'être sanctionné par une condamnation pour crime grave et une peine de trente-cinq ans de prison, ni de faire l'objet d'un procès coûteux, financé lui aussi par les contribuables. Désespéré, anéanti par la poursuite judiciaire, Swartz s'est enlevé la vie le 6 janvier 2013.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Un jour, alors que je discutais du sort de Swartz avec Al-Bassam par messagerie instantanée, j'ai fait mention d'un article du professeur Hal Abelson, qui avait présidé un comité chargé de se pencher sur le rôle du MIT dans cette affaire. Abelson y déchargeait l'institut de toute responsabilité et y affirmait que le jeune homme s'était montré «dangereusement naïf à l'égard de l'exercice [de son] pouvoir [de technicien], au point de s'autodétruire[23]». Consternée, j'avais réagi sur un blog techno populaire: «La vraie naïveté, dans le cas qui nous occupe, est celle d'Abelson. Son refus de dénoncer une poursuite fédérale injuste, violente et excessive, qu'il préfère qualifier de "vigoureuse", est aussi navrant que le choix de cet adjectif, qu'il aurait dû laisser au registre de l'exercice physique[24].» Al-Bassam m'a répondu ceci: «"Dangereusement naïf à l'égard de l'exercice du pouvoir, au point de s'autodétruire" est une affirmation qui devrait s'appliquer à la poursuite, et non à Aaron Swartz.»

Al-Bassam – tflow – a lui-même vécu l'épreuve de la Loi cognant à sa porte après des mois d'action directe pour des causes qui lui tenaient à cœur. Il n'est guère surprenant que la sensibilité propre à la jeunesse soit une source d'énergie politique si créative. Un tel dynamisme peut être difficile à maintenir quand on se heurte à l'affligeante réalité des problèmes qui gangrènent notre monde et que les responsabilités du quotidien prennent de plus en plus de place. Mais si c'est l'idéalisme qui amène des jeunes à prendre le taureau par les cornes, alors nous avons besoin de plus – et non de moins – de «naïveté» juvénile.

Faire voler les stéréotypes en éclat

Adnon, tflow et Slim sont trois militants d'Anonymous. Le collectif n'a rien du *boys' club* d'Américains blancs de la classe moyenne qu'on imagine spontanément. Il n'existe pas de statistiques fiables pour le confirmer, mais les Anons que j'ai rencontrés et ceux qui ont été démasqués en se faisant arrêter composent une faune bigarrée (en passant, l'adjectif *bigarré* rappelle la tenue multicolore de ces *tricksters* qu'étaient les fous du roi). Si l'on

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

ajoute à ces trois hommes la cohorte de hackers avec qui Al-Bassam a travaillé sur #internetfeds (et, plus tard, dans LulzSec), dont les identités sont connues en raison des arrestations, l'hétérogénéité du mouvement devient encore plus manifeste. Leurs rangs comptaient un Portoricain qui habitait un immense HLM de New York (revendeur de drogue à ses heures et père adoptif de ses cousines), deux étudiants irlandais en chimie (dont le radicalisme politique de l'un avait été influencé par son père, un membre de l'Armée républicaine irlandaise (IRA) ayant passé six ans derrière les barreaux), un Écossais qui, pendant la plus grande partie de son engagement dans Anonymous, vivait sur la lointaine île de Yell, et un homme de 35 ans qui, après avoir servi dans l'armée britannique en Irak, s'est lancé en ligne sous le pseudo féminin de Kayla.

Le recours systématique aux pseudonymes, dans ce milieu, a probablement contribué à son cosmopolitisme. Le masquage de marqueurs identitaires comme l'origine ethnique, la classe sociale ou l'âge ouvre une foule de possibilités. Des études ont d'ailleurs confirmé que l'être humain tend à chercher la compagnie d'individus qui lui sont familiers (ou semblables); la camaraderie fondée sur une identité partagée n'a d'ailleurs rien de ridicule et ne doit pas être rejetée par principe[25]. Cependant, il est tout aussi important de créer et de fréquenter des espaces où les marqueurs identitaires sont atténués, afin d'aider à la construction de liens qui, autrement, pourraient ne jamais s'établir. En un sens, pour ce qui est d'Anonymous, il se pourrait que le fait de se définir soi-même comme un membre du collectif suffise, comme identité partagée, à faire émerger et à nourrir de telles relations.

Malgré ces exemples surprenants de diversité, Anonymous est cependant loin d'être un champion de l'hétérogénéité. C'est particulièrement le cas en ce qui a trait au genre: même si le collectif peut se vanter d'avoir eu dans ses rangs des participantes et des organisatrices de premier plan (dont darr, que nous avons présentée dans un chapitre antérieur, et Mercedes Haefer, une militante au caractère bien trempé dont nous examinerons l'activité plus loin), l'unique hacker «femanon» de

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

LulzSec s'est avéré être un individu de sexe masculin se faisant passer pour une femme, Kayla.

La composition d'Anonymous reflète les inégalités structurelles du monde de l'informatique. Or si l'écart entre les sexes s'est amenuisé dans la plupart des domaines liés aux sciences, à la technologie, au génie et aux mathématiques, ce n'est pas la tendance qu'a connue l'informatique. En fait, la marche vers la parité des inscriptions à l'université y a atteint son sommet voilà quelques décennies: en 1985, les femmes obtenaient 37 % des diplômes de premier cycle en informatique, et ce taux se situe aujourd'hui autour de 20 %[26]. En ce qui concerne le milieu des hackers, les données sont rares (vu la nature informelle de bon nombre d'associations), mais tout indique que le taux d'inclusion des femmes y est encore plus bas[27]. Certains secteurs d'activité, tel celui des logiciels libres, ont réagi en adoptant des mesures de promotion de la diversité[28]. Chez les hackers *black hat*, toutefois, les seules femmes que j'ai rencontrées ou dont j'ai entendu parler sont en fait des transgenres, qui, ce qui pourrait en surprendre plusieurs, sont beaucoup plus nombreuses qu'on pourrait le croire. (Inversement, notons que, pour une raison indéterminée, les femmes sont plus répandues dans le milieu des trolls.) Même si aucune recherche en bonne et due forme n'a été menée sur l'underground hacker, on peut présumer que la faible représentation des femmes résulte à la fois de facteurs structurels, des risques judiciaires inhérents aux activités et de l'esprit borné et fanfaron de *boys' club* propre à ce milieu bien établi[29]. Il m'est arrivé à l'occasion d'entendre certains Anons rabaisser la contribution des femmes. Chaque fois, je me suis demandé s'il s'agissait de sexisme ou d'une simple expression de trollage, en sachant très bien que la frontière entre les deux est rarement nette.

En abordant nommément l'enjeu de la diversité et des rapports de genre, on peut poser des questions plus intéressantes encore. Pourquoi, par exemple, les androgynes (*gender benders*), les queers et les femmes trolles sont très bien acceptés, alors que la participation des femmes aux cercles techniques proprement dits reste faible? Certaines identités sont acceptées tandis que d'autres continuent d'être perçues avec méfiance.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Aller au-delà des stéréotypes permet également de mieux comprendre les motivations de bon nombre de ces participants. On peut être en désaccord avec les méthodes utilisées (hacking, attaques par saturation, *doxing*), mais on doit faire la distinction entre les méthodes (et l'importance qu'elles ont) et la composition même d'Anonymous. À maintes reprises, j'ai vu des Anons agir par conviction politique, et certains d'entre eux étaient sans doute de nouveaux venus sur la scène militante.

On perd de vue cette réalité si l'on s'entête à considérer Anonymous à travers le prisme grossier des stéréotypes. Une bonne partie des journalistes qui m'ont interviewée en ma qualité d'«universitaire spécialisée» m'ont demandé, d'une manière ou d'une autre, «quel type de personne semble adhérer à Anonymous». Ma réponse n'est pas de celles qu'on aime entendre, mais je leur dis souvent qu'il n'y en a aucun type en particulier, sinon qu'il s'agit en général de geeks et de hackers. Les gens qui se disent citoyens d'internet affichent une grande diversité d'expériences de vie, de champs d'intérêt et de sensibilités politiques. Pourtant, les journalistes semblent avoir une idée préconçue de l'Anon, qu'ils imaginent en jeune Américain asocial, blanc, en colère, libertarien et membre de la classe moyenne. Ce faisant, on risque beaucoup plus de considérer ses interventions politiques comme juvéniles et louches – fruits de l'angoisse adolescente – que comme l'expression d'un désir d'action fondé sur une véritable conscience politique.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Chapitre 6

Le péril nerd

<Anonymous9> Il y a quelque chose qui me laisse une impression douce-amère en fait
<Anonymous9> Biella est ici pour un projet de recherche universitaire
<Anonymous9> Je ne peux pas m'empêcher de penser que, dès qu'elle aura rédigé sa thèse ou je ne sais quoi, elle n'aura plus de raison de traîner par ici:(
<Anonymous9> Je ne pense pas qu'elle réalise à quel point elle a contribué à Anonymous
<Anonymous9> Même si elle ne considère pas nécessairement qu'elle en fait partie

C'est en 2013 qu'on m'a transmis cet extrait d'une séance de chat remontant à 2011 entre un des principaux organisateurs d'Anonymous et un journaliste. En le lisant, j'ai été submergée par l'émotion et les souvenirs. Ces propos me rappelaient que ma rencontre avec Anonymous s'était inscrite dans une étude de terrain anthropologique on ne peut plus typique, d'abord marquée par un sentiment d'isolement, puis par l'emballement d'avoir trouvé sa place et enfin par les déchirements de l'extraction finale. Anonymous9 avait vu juste: à la suite de l'opération Tunisie, je m'étais investie à fond dans Anonymous, puis, avec le temps, mon engagement avait diminué, en particulier avec la rédaction de ce livre. Après avoir reçu ces lignes, j'ai contacté Anonymous9 – un de mes plus proches confidents

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

du collectif – pour l'assurer qu'il restait mon ami même si j'étais passée à d'autres sujets de recherche (mais seulement à la condition qu'il comprenne que je n'étais plus une étudiante!).

Les propos d'Anonymous9 me rappelèrent aussi que, en un mois seulement, soit en janvier 2011, j'étais passée du statut de profane désorientée à celui de semi-initiée (tout aussi perplexe). Cette évolution est attribuable aux longues heures que je consacrais à la recherche: presque chaque jour, je passais au moins cinq heures en ligne, simultanément connectée à sept, voire à dix canaux Internet Relay Chat (IRC) afin d'observer le va-et-vient des Anons. À cette activité s'ajoutaient les nombreuses interviews que j'accordais aux médias à propos d'Anonymous, lesquelles me demandaient environ dix heures par semaine. En deux ans, j'ai parlé à plus de 150 reporters différents, ce qui m'a valu le douteux record mondial de la personne ayant initié le plus grand nombre de journalistes à l'IRC.

Peu à peu, le vertige ressenti devant la quantité astronomique de données à digérer a laissé place à un sentiment d'appartenance. Je me suis mise à participer aux discussions et me suis fait connaître – et plus ou moins accepter – dans un certain nombre de ces sous-groupes et canaux qui poussaient comme des champignons dans une forêt après l'averse. Après m'être perdue dans les bois, je faisais partie de l'écosystème. Comme dans toute forêt, le danger rôdait par endroits, mais j'ai appris également où se trouvaient les clairières enchantées. Mon port d'attache était un canal IRC d'AnonOps appelé #reporter.

La transition est loin de s'être faite en douceur. J'avais beau me préparer psychologiquement à prendre la parole, à exprimer mon opinion, à me présenter (comme je suis en train de le faire), chaque fois que venait le temps de passer à l'acte, je faisais marche arrière. Pendant des semaines, je suis restée tétanisée par la crainte d'être chassée du canal et de rater ainsi l'incroyable opportunité qu'il représentait. Ces Anons étaient plus farouches et plus bagarreurs que ceux de l'opération Chanology. J'avais vu, littéralement captivée, des membres se faire expulser du canal pour avoir

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

contrevenu à des règles éthiques qui ne m'étaient pas très claires ou, plus terrifiant encore, pour le seul plaisir du *lulz*.

Ce n'est donc pas avant le début de janvier 2011 que j'ai pris la parole pour la première fois. Et je ne l'ai pas fait de façon entièrement volontaire. De manière apparemment inattendue, on a remarqué ma présence. J'observais la scène en toute sécurité, personne ne prêtait attention à moi, puis, soudain, j'ai eu l'impression que l'œil enflammé de Sauron se tournait vers le recoin où j'étais tapie pour en disloquer l'ombre et m'inonder de sa lumière vive. Je m'étais éloignée de l'ordinateur pour aller chercher à manger dans la cuisine. À mon retour, j'ai trouvé ceci sur mon écran:

> <Topiary> Quelqu'un peut-il confirmer l'existence de biella?
> <q> je lui ai parlé aujourd'hui, mais...
> <m42> tu la connais, q?
> <q> si elle m'envoyait un DM [message privé] par twitter, je pourrais.
> <m42> «biella n'est pas ici pour le moment», et pas de @ dans aucun des 7 canaux
> <q> oui, si elle est la biella de twitter, je lui ai déjà parlé
> <Topiary> Nous devrons peut-être chasser les journalistes d'ici dans un moment
> <m42> elle peut revenir plus tard
> Vous avez été chassé du canal par q: (salut biella, peux-tu m'envoyer un DM sur twitter stp? Merci!)

Mon cœur battait la chamade et je maugréais. Se faire chasser d'un canal est très contrariant. On ne peut plus voir ce qui s'y passe et on ne connaît jamais les raisons d'une éviction sommaire contre laquelle on n'a pu se défendre. C'est plutôt embarrassant: la personne expulsée ne peut que se demander ce que les gens disent d'elle en son absence et elle ignore si elle sera réadmise. Elle peut être frappée d'une «Q-line» ou, pire encore, d'une «Z-line», par laquelle un administrateur bannit une fois pour toutes son adresse IP de l'ensemble du serveur, c'est-à-dire de tous les canaux à la fois. Mais, heureusement, ce n'est pas ce que les Anons avaient en tête. Ils

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

ne m'avaient pas chassée du canal pour de bon. Au bout de dix minutes, tourmentée par l'anxiété, j'ai pu me reconnecter:

<biella> salut q Topiary
<biella> désolée j'étais en train de faire la cuisine
<biella> c'est moi
<biella> http://steinhardt.nyu.edu/faculty_bios/view/Gabriella_Coleman
<biella> j'ai envoyé beaucoup de journalistes ici
<biella> et j'écris et je donne des conférences sur Anonymous

Ils se sont empressés de répondre:

<Topiary> Salut biella, désolé de t'avoir expulsée
<biella> c'est pas grave
<biella> vous m'aviez bien prévenue:-) et je suis restée trop longtemps inactive
<biella> plus longtemps que je l'aurais souhaité
<Topiary> On a simplement l'habitude d'être très stricts et parfois un peu paranoïaques avec les utilisateurs inconnus qui se pointent ici
[...]
<Topiary> Ça m'a plu ce que j'ai lu sur ton lien. Tu aborderas quels aspects d'Anonymous dans ton exposé?
<q> biella, peux-tu m'envoyer un DM sur twitter?
<Topiary> En tout cas je serai ravi de lire tes travaux.
<biella> cool Topiary et je commencerai par le point 1: si je me trompe/suis à côté de la plaque contactez-moi svp. Je suis toujours ouverte aux remarques
<biella> q, quel est ton compte twitter?
<biella> le mien https://twitter.com/#!/BiellaColeman [...]
<biella> contente que tu l'aies, et je ne traînerai plus ici sans raison aussi souvent

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<biella> ok je vous laisse et je reviendrai quand j'aurai des questions. j'ai déjà des questions mais tout le monde me harcèle pour que j'aille dîner
<Topiary> Tu sembles avoir les pieds sur terre, heureux de constater que tu t'intéresses à nous. Bon appétit.
<Trivette> d'accord
<biella> merci Topiary, ok on se reparle plus tard
<q> ouais, je n'ai que de bonnes choses à dire sur biella. je voulais juste m'assurer que c'était la même:)

Ouf! En y repensant, je dirais plutôt OUUUFFFFFF! C'était un moment décisif. S'ils m'avaient trouvée nulle ou indigne de leur confiance, ils auraient signé la fin de mon projet, ou, à tout le moins, accéder à leur univers aurait représenté pour moi une tâche digne des travaux d'Hercule. Les membres de #reporter ont une autorité plus grande que celle de l'Anon moyen. Leur opinion compte.

Le récit de mon adoption sans douleur mérite probablement d'être raconté plus en détail. Rappelons que j'ai passé deux ans à faire des recherches sur l'opération Chanology. Bien que les cultures d'AnonOps et des militants anti-Scientologie soient différentes l'une de l'autre, elles sont assez apparentées pour que mes travaux aient touché une corde sensible chez les membres qui les ont consultés. En écoutant mes conférences vidéo, en particulier, on se rendait vite compte que j'éprouvais de la sympathie pour Anonymous – ou à tout le moins que j'appréciais le *lulz*.

Et je n'étais pas la seule. Une demi-douzaine de gens de l'extérieur s'étaient vu accorder un accès privilégié en contrepartie de leur engagement à relayer Anonymous dans les médias. Pour *The Tech Herald*, le hacker devenu reporter Steve Ragan a pondu les articles les plus fouillés et les plus nuancés jamais publiés sur le collectif. Avec ses nombreux reportages sur Anonymous dans *Forbes*, Parmy Olson est en quelque sorte devenue la journaliste attitrée de LulzSec. Deux membres, Sabu et Topiary, se sont confiés à elle en allant jusqu'à admettre – chose quasi incroyable – avoir commis des actes illégaux. Pendant la campagne Occupy, où Anonymous

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

s’est solidarisé avec les 99 %, Quinn Norton a publié de longs articles très remarqués dans *Wired*. Pour un long métrage documentaire, le cinéaste Brian Knappenberger a passé plus d’un an à interviewer sans relâche plus de 40 Anons sur IRC, par chat vidéo ou en personne. (Brian et moi ferions équipe en vue de rechercher Sabu pour le filmer, une entreprise qui se solderait par un échec lamentable.) Asher Wolf, une geek d’exception, a discuté en coulisse avec de nombreux Anons et a réussi comme nul autre à saisir leur esprit de corps dans ses messages de 140 caractères publiés sur Twitter. Alors qu’elle collaborait à CNN, Amber Lyon s’est démarquée en réalisant le projet qui, de tous ceux que nous avons menés, s’est avéré le plus éloigné d’internet: elle a franchi un col reculé séparant l’État de Washington de la Colombie-Britannique à pied, en compagnie du hacker d’Anonymous Commander X (Christopher Doyon), qui s’enfuyait des États-Unis pour éviter la prison.

Les relations d’Anonymous avec les médias sont tout aussi contradictoires et hétéroclites que le collectif lui-même. La plupart des participants collaborent avec les journalistes avec autant de respect et de transparence que le permet l’impératif de clandestinité. En général, leur principal objectif consiste à faire connaître leurs causes, comme ce fut le cas lors de la contestation en Tunisie, mais ils cherchent aussi, autant que possible, à soigner leur image. En quelques rares occasions, ils ont voulu troller certains journalistes.

La gestion de l’image comme le trollage sont gérés par des spécialistes «maison» de la com’, qui excellent dans l’art d’adapter le contenu à l’un ou l’autre de ces buts. Sur #reporter, ces derniers se mêlaient aux journalistes et aux visiteurs comme moi, et deux d’entre eux étaient réputés pour s’adresser à la presse avec panache: Topiary, qui, finirait-on par apprendre, était en fait Jake Davis, 18 ans, citoyen des lointaines îles Shetland en Écosse (dans sa notice biographique sur Twitter, il se qualifiait de «simple clown devenu chic haie de jardin» – *topiary* se traduit par «topiaire»), et Barrett Brown, un Texan à la peau claire et aux cheveux roux dont le salon jonché de livres était orné d’un lynx empaillé. Pendant l’opération Tunisie, tflow avait convié Topiary au Saint des saints, et celui-ci s’était révélé

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

tellement habile à produire et à diffuser une exquise propagande imprégnée de l'esprit du *lulz* qu'il en était devenu un des principaux membres. Quant à Brown, c'est après un court article qu'il avait rédigé faisant l'éloge d'Anonymous que Gregg Housh, un des membres fondateurs de marblecake, l'avait recruté.

Topiary et Barrett Brown étaient aussi les *tricksters* en résidence d'AnonOps: chacun d'eux avait développé sa marque personnelle en matière de bouffonnerie. Inspiré par Dada et l'Internationale situationniste, dont l'humour corrosif avait marqué l'avant-garde artistique au XX^{e} siècle, Topiary était passé maître dans l'art de manipuler les médias par l'absurde avec ses messages à la fois géniaux et insensés de 140 caractères. Sur le canal #reporter, il n'hésitait pas à vanter ses propres exploits et à en planifier d'autres en direct:

> <Topiary> À eux, je leur ai déjà accordé une interview audio, ils sont bons, ils passent par Skype
> <Topiary> Je leur ai dit qu'on avait plus de 9 000 membres, je les ai menés en bateau, vous devriez les faire tourner en bourique
> <Topiary> Ou un truc du genre
> <Topiary> Bref, je viens d'achever une conversation avec Andy, un homo invraisemblable qui est en train d'écrire un papier sur nos dernières conneries par fax

Admiré de nombreux Anons, Topiary le plaisantin avançait masqué: comme presque tous ses semblables, il utilisait un pseudo. Son vrai nom ne serait révélé qu'au moment de son arrestation. En revanche, si je n'ai pas encore mentionné le pseudo de Barrett Brown, c'est qu'il n'en avait pas. Il était tout simplement Barrett Brown – parfois à demi nu, comme nous le verrons, mais toujours Barrett Brown. Porte-parole d'Anonymous pendant l'hiver 2011, il occuperait cette fonction jusqu'à ce qu'une vague de mécontentement le pousse vers la sortie, en mai. Il jouait aussi le rôle de bouffon d'AnonOps. Comme tout *trickster* qui se respecte, il savait apprécier un bain moussant très chaud assorti d'un verre de rouge (sans doute bon marché). Une fois ses intentions annoncées sur Twitter («Vais me

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

servir un verre de rouge; prendrai un bain moussant en direct dans un quart d'heure[1]»), les spectateurs pouvaient se connecter à Tinychat (un service de chat vidéo) pour le voir installé dans sa baignoire, l'insulter et lui lancer des blagues de mauvais goût qui, dans son cas, prenaient la forme de blagues de viol.

Arrivé avec son nom, donc, il serait chassé sans cérémonie – toujours avec son nom – pour avoir enfreint une des règles de base d'Anonymous (le nom du collectif donne une idée de la règle): le tabou, l'interdiction absolue de rechercher attention et célébrité. En jouant les iconoclastes, Brown avait cherché à occuper une position intermédiaire, d'entre-deux. Il se comportait comme un initié, mais sans jamais se dissimuler. Il semble avoir été toléré aussi longtemps parce qu'il apportait une contribution précieuse, tant au réseau qu'à la cause. Journaliste de formation, il excellait à accabler les puissants par ses écrits ironiques, parodiques et cinglants. Par exemple, dans un texte paru dans *Vanity Fair* où il faisait l'éloge du journaliste d'enquête (aujourd'hui décédé) Michael Hastings (le portrait peu flatteur qu'avait fait Hastings du général américain Stanley McChrystal pour *Rolling Stone* avait entraîné la chute de ce dernier), on pouvait lire: «Il aurait mieux valu pour McChrystal qu'il parle à Thomas Friedman, qui, en 2001, avait fait montre d'une telle naïveté lorsqu'il avait déclaré que Vladimir Poutine incarnait une force du bien que tous les Américains devraient soutenir (*rootin'*), un mot qu'il avait choisi parce qu'il rime avec Poutine[2].» Brown, qui avait un sens aigu des médias, offrait librement ses conseils aux autres Anons. Dans une interview, un Anon chargé d'écrire des communiqués de presse l'a évoqué ainsi: «C'est Barrett qui m'a appris à capter l'attention des journalistes, à diffuser des [communiqués], à jouer avec le cycle des nouvelles, à choisir le bon moment et plein d'autres trucs.» Mais les pitreries de Barrett, conjuguées à son rôle d'attaché de presse, cadraient mal avec l'éthique d'Anonymous. C'est ainsi qu'AnonOps a fini par bannir son fou du roi.

L'autopromotion n'est pas tolérée

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

À la mi-décembre 2010, le journaliste Ian Shapira, du *Washington Post*, m'a contactée. Je lui ai fait un résumé de l'histoire d'Anonymous et l'ai encouragé fortement à se connecter à IRC, en particulier au canal #reporter, pour le reportage qu'il était en train d'effectuer. J'ignore s'il y est allé, mais, le 22 janvier 2011, il a publié un article substantiel qui mettait en scène un membre d'AnonOps de la région de Washington:

> Il a adopté le nom de code AnonSnapple pour dissimuler son appartenance à un collectif de cybervoyous et d'activistes appelé Anonymous. Peu d'élèves de l'école privée qu'il fréquente à Washington savent que ce jeune homme de 17 ans participe aux manifestations publiques d'Anonymous, où il arbore le rictus moustachu du masque de Guy Fawkes, emblématique du mouvement. [...]
>
> AnonSnapple, qui habite près de Bethesda avec sa mère, femme au foyer, et son père, économiste au Fonds monétaire international, craint que des enquêteurs ne l'associent aux attaques par saturation lancées le mois dernier par des membres d'Anonymous contre MasterCard, Visa et PayPal, qui avaient cessé de traiter les paiements à WikiLeaks. «Il y a un certain temps, le FBI s'en est pris aux serveurs d'Anons qui avaient pris part aux attaques», a-t-il expliqué. «Même si je n'y ai pas participé, je fais toujours partie du collectif. Je fréquente toujours les mêmes forums que ceux qui [ont mené] les attaques par saturation. [...] On pourrait facilement m'associer à eux[3]».

Le 25 janvier, quelques jours après la parution de l'article, j'ai envoyé le lien sur #reporter. C'était une période où la routine suivait son cours sur le canal, on y discutait de choses et d'autres. Les participants se sont jetés sur le texte comme une meute de chiens sur un os. En quelques minutes, les foudres de l'enfer se sont déchaînées. Pendant une heure environ, le tumulte a secoué différents canaux, notamment #reporter et #lounge:

> <shitstorm> snapple a l'air d'avoir agi tout seul

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<shitstorm> sur une interview locale par exemple
<biella> j'ai essayé de le convaincre de se connecter à l'irc, mais je crois qu'il ne l'a pas fait, et ça se voit
<shitstorm> Cette interview est ridicule, on dirait une publicité pour snapple
<shitstorm> du «namefagging»
<shitstorm> J'ai fait ceci
<shitstorm> J'ai fait cela
<owen> c'est clair
<q>:/
<shitstorm> C'est débile en fait
<shitstorm> Je suis furieux
<owen> je vais le bannir
<owen> partout
<shitstorm> excellent
<owen> des conneries opportunistes
<shitstorm> «Il est terrifié par l'idée de voir son identité révélée.»
<shitstorm> T'AS QU'À PAS DONNER TOUS CES DÉTAILS

La conversation qui se déroulait sur mon écran était empreinte d'un mépris féroce. Les propos étaient durs. Je comprenais pourquoi ces Anons étaient en colère, mais j'avais eu affaire à suffisamment de journalistes pour les inciter à la prudence:

<biella> avant de le [snapple] mettre dehors, assurez-vous que le journaliste n'a pas tout déformé (à moins que ce soit habituel)
<owen> j'en ai tellement marre de ces gamins qui pensent que tout ça c'est qu'un jeu en plus grand
<q> il a sûrement déformé tout le truc
<biella> qui sait si mes mots ne viennent pas d'être gravement gravement déformés?
<q> et je ne pense pas que ian ferait une telle chose
<q> c'est un journaliste sérieux
<owen> ça ressemble beaucoup à snapple selon moi

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<shitstorm> suis d'accord
<biella> ok, vous savez certainement ce qu'il y a de mieux à faire

Même si les Anons collaborent parfois de façon sérieuse avec les journalistes, il leur arrive aussi de les troller ou de les tailler en pièces (oui, même les «journalistes sérieux»). Ce n'est cependant pas ce qu'ils ont fait dans ce cas. Ils étaient surtout contrariés par le fait qu'AnonSnapple, qui n'avait jamais pris le moindre risque pendant une opération, parle au nom de ceux qui en avaient pris:

<owen> il connaît rien à rien
<owen> il doit foutre le camp
<owen> n'est-il pas l'un des vôtres, q?
<shitstorm> Y a pas longtps, AnonSnapple a demandé à un prof s'il pouvait comptabiliser les heures qu'il avait passées à concevoir et à distribuer des dépliants pour un rassemblement d'Anonymous à Dupont Circle.
<shitstorm> TU TE FOUS DE MA GUEULE?
<shitstorm>!!!!!!!!!!!1
<shitstorm>! c'est hallucinant
<owen>! je veux le savoir s'il se pointe ici svp
<owen> petits merdeux...
<shitstorm> je veux l'étrangler
<shitstorm> aussi

L'étrangler. C'est à peu près ce qu'ils ont fait. Les Anons ont convoqué AnonSnapple sur le canal:

<shitstorm> putain Snapple
<shitstorm> qu'as-tu fait
<shitstorm>?
<shitstorm> Snapple ça doit être la pire connerie, pire que prie
<shitstorm> pire*
<q> impressionnant
<owen> snapple

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<owen> maintenant parle
<shitstorm> Snapple
<shitstorm> Snapple
<owen> avant que je te vire d'ici
<shitstorm> Snapple
<Nessuno> Snapple est silrnciux
<Nessuno> silencieux*
<shitstorm> parce qu'il sait qu'il est dans le caca
<Snapple> hahahaa
<shitstorm> ah salut
<Snapple> croyez-moi, ces conneries c'est qu'à moitié vrai
<MTBC> zut il sait qu'il a fait de la merde
<owen> tu trouves ça drôle?
<Nessuno> là, en plein merdier justement
<shitstorm> Snapple, pourquoi ce serait pas vrai?
<owen> attends
<shitstorm> ça semble correspondre exactement à ce que j'ai vu et entendu
<owen> tu dis qu'ils ont MENTI?
<owen> JE LES EMMÈNE ICI DE SUITE
<Snapple> Parce que je dirais jamais où j'habite
<owen> et on verra
<Snapple> D'abord
<Snapple> ni ce que font mes parents
<shitstorm> mais tu nous dis que tu es à washington
<owen> tu le ferais si tu voulais être célèbre
<Snapple> J'habite à Washington
<shitstorm> sans dec'
<Snapple> C'est tout
<owen> on sait tous où t'habites
<shitstorm> ^
<Snapple>:)
<owen> tu le dis à tout le monde

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<Snapple> venez
<shitstorm> d'accord
shitstorm prend le fusil d'assaut
<shitstorm> owen, on y va?
<Snapple> *part en courant*
<shitstorm> Master-IT amène le M16
MTBC saisit le fusil d'assaut et se tire dans le visage
Snapple a quitté le salon (une Z-line (crétin)).

La colère à l'égard d'AnonSnapple était si profonde et si vive que même son bannissement (un mécanisme de largage habituellement efficace) n'a pas suffi à chasser les nuages noirs. Les Anons fulminaient encore. Les vacheries fusaient de tous les côtés (owen, par exemple, lança qu'«en attendant, ce soir snapple pourra faire sagement ses devoirs au lieu d'aller sur IRC»). Après les avoir informés que je connaissais le journaliste, je me suis mise au travail:

<biella> owen, q, je connais ian
<q> tu l'as dit sur reporter
<q> biella, tu peux nous aider?
<biella> bien sûr je peux lui parler de l'affaire ou lui dire qu'il devrait voir avec q

Finalement, sur un autre canal, owen conclut par quelques observations:

<owen> je ne tolérerai plus que quiconque tente d'utiliser le travail accompli par tant de monde pour se mettre en avant personnellement
<Nessuno> owen a bien raison
<owen> il a dit «hé, regardez-moi mais j'ai rien fait du tout»
<butts> j'arrive pas à croire qu'il lui ait raconté tout ça
<owen> qu'il aille se faire foutre

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Insulter le chasseur

Ce dont j'ai été témoin m'a abasourdie. Certes, j'étais au courant de la prohibition touchant le *namefagging* (le fait pour un Anon d'associer son identité à ses actes). Solidement ancrée et rarement transgressée (notons que Barrett Brown serait bientôt vilipendé pour son comportement, somme toute similaire à celui d'AnonSnapple), cette règle remonte à l'époque où Anonymous n'était pas encore un groupe militant. Mais je n'avais jamais assisté à son application en temps réel. L'affaire m'apparaissait d'autant plus captivante qu'elle me donnait enfin l'occasion d'être témoin d'un phénomène que je ne connaissais alors que par mes lectures de récits ethnographiques. Très répandues, les méthodes destinées à faire respecter l'idéal de l'égalité varient selon les cultures. Elles peuvent aller jusqu'à ruiner la vie d'une personne (pensons à l'accusation de sorcellerie) ou être relativement anodines, mais toutes sont assez efficaces. Un de mes exemples favoris vient du peuple des !Kung San, des Bochimans vivant dans le désert du Kalahari, en Afrique. Quand des chasseurs ramènent une énorme pièce de viande au village, on ne les couvre pas d'éloges (comme on pourrait s'y attendre des membres d'une tribu qui adore la viande), mais plutôt d'insultes. Cette moquerie permet de tempérer leur orgueil:

> Quand un homme bochiman revient de la chasse, il ne doit pas rentrer chez lui en faisant le fanfaron: «J'en ai tué un gros dans le bois!» Il doit d'abord s'asseoir en silence jusqu'à ce que quelqu'un s'approche de son feu et lui demande: «Qu'as-tu vu aujourd'hui?» Il répond calmement: «Ah, je ne suis pas doué pour la chasse. Je n'ai rien vu du tout... Juste une toute petite bête.» Je ris dans ma barbe, poursuit /gaugo, car je sais qu'il en a tué une grosse.
>
> Au matin, nous formons un groupe de quatre ou cinq personnes pour couper la viande et l'apporter au camp. Rendus à l'endroit où se trouve la proie, nous l'examinons, puis nous nous écrions: «Tu nous as traînés jusqu'ici pour nous faire transporter ce sac d'os chez toi? Si

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> j’aurais su, j’aurais pas venu!» Un autre membre de la tribu donne son opinion: «Les amis, quand je pense que j’ai renoncé à une belle journée à l’ombre pour ça! Au village, nous sommes peut-être affamés, mais au moins nous avons de l’eau fraîche[4].»

Ce type de nivellement moral n’élimine pas les rapports de pouvoir, encore moins les inégalités. Certains individus sont tout simplement meilleurs chasseurs que d’autres. Sur IRC, ce sont des Anons comme owen ou shitstorm qui mènent la barque, et leur savoir-faire technique leur confère manifestement l’autorité de faire respecter les normes. Bannir des gens d’un réseau IRC après les avoir abreuvés d’insultes n’engendre pas un égalitarisme strict, mais permet simplement de minimiser l’importance des rapports de pouvoir et de les moduler. Si, dans une certaine mesure, les Anons acceptent de se féliciter entre eux, ils réprouvent toute tentative de faire rayonner à l’extérieur de leur milieu une réputation acquise en interne. Pour assurer la notoriété d’Anonymous en tant que collectif, l’individualité et l’image publique d’un membre ne peuvent faire partie de l’équation.

Si AnonSnapple avait participé plus activement aux opérations (en particulier s’il avait pris le risque de la désobéissance civile), je crois qu’il s’en serait tiré avec une simple réprimande au lieu d’être banni. Parce que le jeune homme prétendait en avoir fait assez pour craindre les autorités en dénigrant du même souffle les tactiques hardies de ses camarades, son entreprise d’autoglorification a été perçue comme un affront de premier ordre. À ce moment-là, les Anons étaient déjà très conscients des éventuelles conséquences judiciaires de leurs actes (deux jours plus tard seulement, dans la foulée d’une récente campagne d’attaques par saturation, des arrestations auraient lieu au Royaume-Uni et des mandats seraient lancés aux États-Unis). On a condamné AnonSnapple parce qu’il avait agi dans son propre intérêt, et des dizaines de personnes se sont connectées à #lounge pour assister à l’exécution en mangeant du popcorn. Mais il ne s’agissait pas d’un simple divertissement. La correction a représenté une leçon de morale sans équivoque pour les observateurs, qui l’ont tacitement approuvée par leur silence.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Le péril nerd

Le jour même du renvoi d'AnonSnapple, j'ai été de nouveau saisie par le vertige devant une incroyable succession d'événements ayant eu lieu au sein comme à l'extérieur d'AnonOps. Pendant les deux semaines qui ont suivi, j'ai passé le plus clair de mon temps en ligne à observer Anonymous prendre part à une révolution historique. De plus, en composant avec la première vague d'arrestations à frapper leur réseau, les Anons ont planifié et exécuté un acte de vengeance d'une ampleur inouïe.

Le jour, donc, où AnonSnapple fut sommé de gravir le mont Olympe pour y subir son rituel d'exclusion, la secrétaire d'État des États-Unis, Hillary Clinton, émit une déclaration sur le soulèvement populaire qui secouait l'Égypte: «[À] notre avis, le gouvernement égyptien est stable et tente de trouver les moyens de répondre aux besoins et aux intérêts du peuple égyptien[5].» Inspirés par la révolution tunisienne, les Égyptiens manifestaient depuis début janvier pour réclamer la démission du dictateur Mohammed Hosni Moubarak, au pouvoir depuis trente ans. Les organisateurs avaient appelé à faire du 25 janvier une journée de révolte. Les manifestants affluaient en masse. Alors que les événements se précipitaient, le tout nouveau canal #OpEgypt fut transporté par l'enthousiasme et un sentiment d'horreur (les pseudos ont été modifiés):

<WebA18> oui, twitter est censuré en égypte
<WebA18> et ils essaient de censurer facebook
<0n> les téléphones portables aussi
<t23> n'étant pas en égypte, je ne peux pas vous le confirmer à 100 %
<0n> C'EST LA PANIQUE
<t23> mais c'est une tactique connue
<WebA18> un ami égyptien me dit qu'on le censure
<eb> si ça vous chante, vous pourriez manifester à l'ambassade égyptienne

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<Ion> CONNECTEZ-VOUS À #propaganda POUR CONCEVOIR ET CRÉER DU MATÉRIEL POUR #opegypt
<jeb> pour attirer l'attention des médias et appuyer nos /b/ons amis égyptiens
<WebA18> merci!
<mib> Les manifestations s'étendent et prennent de l'ampleur
<bi> Les Égyptiens ont des couilles de fer. GO GO GO!
<pi> est-ce qu'il y a un mode ruche auquel je pourrais contribuer?
<mib> nous ne devons pas nous arrêter avant que le régime tombe [...]
<b> Diffusez ce FLYER pour RECRUTER plus de monde: http://i.imgur.com/LfLhN.png

Le gouvernement avait d'abord perturbé les systèmes de communication de façon sporadique, mais, le 28 janvier, il mit le paquet en coupant l'accès à internet au pays entier.

En vue de rétablir un minimum de connectivité en Égypte, Anonymous s'associa à un autre collectif de hackers militants, Telecomix. Les deux groupes avaient connu des divergences dans le passé. Opposé aux attaques par saturation, Telecomix avait tenté de maintenir en fonction des sites qu'Anonymous cherchait à bloquer. Néanmoins, quand un problème s'avérait assez urgent et stimulant (comme la nécessité d'aider des gens dans le besoin à avoir accès aux réseaux de communication), les hackers savaient mettre leurs différends de côté pour travailler de concert. Des Anons contribuèrent ainsi à l'effort entrepris par Telecomix pour trouver un moyen de connecter l'Égypte à internet de façon détournée, à l'aide de modems, de fax et de téléphones obsolètes. Au même moment, la petite élite technicienne d'Anonymous, qui, en se regroupant dans le cadre de l'opération Tunisie, avait créé un canal IRC permanent, poursuivait ses hackscapades en soutien au Printemps arabe.

Alors que l'opération Égypte prenait son essor contre le gouvernement Moubarak, les Anons eux-mêmes faisaient face à une menace. Deux jours

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

après le bannissement de Snapple et la journée historique de révolte du peuple égyptien, une alerte apparut sur #reporter, en gros caractères rouges:

> <ew> ATTENTION: Aux Anons américains et britanniques qui ont participé aux attaques contre MasterCard, Visa ou la BOA [Bank of America], effacez immédiatement de vos machines toute donnée qui pourrait vous associer à ces opérations!

Le 27 janvier, en effet, les autorités britanniques avaient appréhendé des participants présumés, et, aux États-Unis, 3 agents du Federal Bureau of Investigation (FBI) avaient émis 40 mandats d'arrestation relatifs aux attaques par saturation menées dans le cadre de l'opération Payback (lesquels mèneraient à l'arrestation d'un groupe de 14 Anons):

> <Anonymous9> Salut les amis
> <Anonymous9> J'imagine que vous avez entendu la nouvelle?:(
> <shitstorm> oui
> <shitstorm> triste journée
> <Anonymous9> les gouvernements viennent de descendre encore plus bas
> <Anonymous9> Déprimant en effet
> <Anonymous9> Mais, en toute justice, pas inattendu
> <shitstorm> c'est pas faux
> <Anonymous9> Ouais
> <shitstorm> mais ils n'ont pas une foutue preuve encore
> <Anonymous9> C'est fascinant de voir à quel point ils nous pourchassent sans merci
> <Anonymous9> Pendant que les vrais criminels nommés dans les câbles diplomatiques de WikiLeaks sont défendus par leurs gouvernements respectifs
> <Anonymous9> Il y a quelque chose de vraiment malsain dans tout ça
> <shitstorm> t'as bien raison

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> <Anonymous9> Ils peuvent dire ce qu'ils veulent, on n'a jamais trempé dans des cas de torture ou de meurtre
> <Anonymous9> Et ça les empêche pas de dépenser des montagnes de fric pour envoyer des gens après nous
> <Anonymous9> Pendant qu'ils filent l'immunité diplomatique etc. aux responsables des crimes les plus graves

Ainsi Anonymous9 prenait-il acte des premières mesures répressives à grande échelle lancées contre Anonymous, avec une condamnation bien sentie de l'hypocrisie du pouvoir d'État. Depuis ce premier coup de filet, plus d'une centaine d'autres personnes ont été arrêtées un peu partout dans le monde, de l'Indonésie aux États-Unis, en passant par la République dominicaine et le Cambodge. Cette vague d'arrestations exceptionnelle représente un point culminant de l'histoire du hacking. Jamais autant de hackers et de geeks n'ont été appréhendés pour leurs idées et leurs actions politiques dans une rafle coordonnée à l'échelle de la planète. Dans les années 1980, 1990 et 2000, des dizaines de hackers ont été arrêtés, mais les raids étaient plutôt sporadiques et prenaient l'une ou l'autre des deux formes suivantes (j'exclus ici les hackers arrêtés pour des actes purement criminels comme la fraude bancaire[6]). Soit les autorités s'en prenaient à des hackers en particulier, comme ce fut le cas pour Kevin Mitnick ou Gary McKinnon, dont l'activité ne visait pas le changement social mais leur intérêt personnel, soit elles attaquaient des groupes de hackers marginaux en vue de les faire taire et de démanteler leurs lieux de réunion (tels que les forums). De tous ces raids, le plus célèbre est sans conteste l'opération Sundevil (bouton d'herpès), menée le 8 mai 1990 dans 14 villes des États-Unis, pour laquelle on a lancé 27 mandats de perquisition et procédé à 4 arrestations[7]. Parfois, comme ce fut le cas du jeune Julian Assange, des hackers qui avaient mis leurs compétences au service d'objectifs politiques larges faisaient l'objet d'accusations criminelles, mais de telles interventions étaient assez rares.

Anonymous est donc le premier grand mouvement de hackers militants à avoir fait l'objet d'une vaste campagne de répression coordonnée

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

impliquant plusieurs États. Le collectif s'inscrit parfaitement dans ce que Gráinne O'Neill, avocate ayant défendu bon nombre d'individus arrêtés pour le compte de la National Lawyers Guild (une association américaine de juristes progressistes), a judicieusement qualifié de «péril nerd» (*nerd scare*).

Veuillez prendre place

Depuis cette époque, j'ai rencontré et interviewé plusieurs personnes prises pour cible dans le cadre du «péril nerd», mais c'est le récit de l'une d'elles, Mercedes Haefer, qui m'a le plus marqué. Haefer s'est jointe à AnonOps en novembre 2010. Alors âgée de 19 ans, elle s'est vite hissée au premier plan grâce à sa vivacité d'esprit et à son intelligence. La jeune femme est une professionnelle dans l'art de la répartie, elle n'a pas la langue dans sa poche. J'ai fait une table ronde avec elle lors de l'édition 2012 du DEF CON, le plus important congrès de hackers au monde. Avant d'entreprendre le récit à la fois sérieux et passionné de son engagement dans Anonymous, elle a demandé au public (à 99 % masculin) de «sortir leurs nichons ou de foutre le camp»: «*Tits or gtfo*» [«Nichons ou fous le camp»] est un commentaire désobligeant qui, dans certaines communautés virtuelles, fuse aussitôt qu'une participante indique qu'elle est une femme.

Comme chaque année, le DEF CON se tenait à Las Vegas, où vit Haefer. Son logement étant assez éloigné de l'immeuble où avait lieu le congrès, je lui ai offert de partager ma chambre d'hôtel, mais à une condition: que weev, l'inimitable troll des trolls, ne s'en approche pas. Il avait fait des avances à Haefer sur Twitter, et on l'avait aperçu au congrès; or j'avais beau être enchantée à l'idée de passer un moment en sa compagnie, et ne voir aucun inconvénient à ce que les deux hackers se rapprochent et plus si affinités, je ne pouvais supporter la perspective de voir un enfant troll répugnant surgir des gouffres de l'enfer en conséquence d'une infâme communion charnelle célébrée dans *ma* chambre d'hôtel (trop grande responsabilité, et je ne connais pas assez d'exorcistes).

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Haefer a obtempéré, et nous nous sommes lancées dans d'innombrables discussions, qui se sont poursuivies en ligne par la suite. Sachant qu'elle avait été prise dans une des rafles qui avaient eu lieu peu de temps auparavant, je lui ai demandé comment on se sent quand le FBI débarque chez soi. Son histoire vaut la peine d'être racontée, car il est bien commode d'avoir une idée de la façon dont ces visites se passent si l'on court le risque d'en subir une. La plupart des gens que j'ai interviewés étaient mal outillés lorsqu'ils ont fait face à ce genre de démonstration de force subite et intimidante; ils ont parlé, alors qu'ils auraient dû garder le silence sauf pour réclamer la présence d'un avocat. «Les gens paniquent, les gens paniquent [...], et les autorités comptent là-dessus. Elles n'attendent que cela. C'est ce qui leur permet de recueillir un maximum de renseignements», avait lancé Emmanuel Goldstein lors du panel de triste mémoire sur la délation au forum Hackers on Planet Earth (HOPE). (Notons que le récit qui suit repose sur le témoignage d'une seule personne et constitue donc sa version des faits. Néanmoins, de nombreux détails importants concordent avec les descriptions contenues dans un document du FBI intitulé *FD-302*, qui résume les interrogatoires et dont j'ai obtenu copie.) Voici le récit en question.

Le FBI débarqua à l'aube. Haefer dormait paisiblement dans son appartement d'un quartier ouvrier de Las Vegas quand un groupe de cinq à huit policiers s'est approché discrètement dans l'aurore hivernale du désert. (Elle a peiné à se souvenir du nombre précis d'agents parce qu'elle était endormie; ils «se ressemblaient tous», m'a-t-elle dit.) Le silence se rompit lorsqu'ils cognèrent à la porte. Brusquement tirée de son sommeil, elle ne fut pas effrayée, car elle se dit que son père, dont les horaires de travail étaient atypiques, avait sans doute oublié ses clés. Elle se traîna hors du lit pour se rendre à la porte en pyjama; en l'ouvrant, elle fut «aveuglée par une lampe de poche, ce qui, à six heures du matin, déstabiliserait n'importe qui». La situation se révéla encore plus déroutante lorsque Haefer réalisa que six carabines étaient pointées vers elle.

Les policiers la sortirent de l'immeuble pour l'emmener dans le passage qui traverse le complexe d'habitations, puis commencèrent à la

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

fouiller. Ce faisant, ils lui posèrent diverses questions afin de confirmer son identité, jusqu'à ce qu'elle sorte de sa torpeur et rétorque: «C'est moi, idiot. Dégage. Je rentre. On se gèle.» Une fois cette formalité accomplie, tout le monde se réfugia dans la chaleur de l'appartement.

Un policier lui demanda si elle voulait s'asseoir. Doutant de la sincérité de l'agent, la jeune femme eut l'impression qu'il faisait étalage de son pouvoir. «On n'offre pas à quelqu'un de s'asseoir dans sa propre maison», m'a-t-elle expliqué. Ce geste autoritaire suscita chez elle une prise de conscience: «Ces gens n'étaient pas mes amis. Ils n'allaient pas m'aider. Ils étaient là pour le boulot.»

Les policiers fouillèrent la maison, se saisirent de photos dans les cartes mémoires des appareils qu'ils trouvèrent, confisquèrent l'ordinateur puis se mirent à interroger Haefer. Elle m'a dit lors de notre rencontre qu'il lui arrivait d'être effrontée, et la suite du récit le confirme. Comme le veut le protocole en vigueur au FBI, l'interrogatoire fut mené par deux agents, un qui posait les questions et l'autre qui notait les réponses[8]. Ils lui posèrent des questions sur 4chan («Si vous croyez qu'il est question de 4chan, vous êtes encore plus incompétents que je le croyais», pensait-elle.) Elle se mit alors à déblatérer sur «ce fil de discussion où il était question d'un type qui était amoureux de sa chienne et voulait la mettre enceinte; il avait recueilli des échantillons qu'il avait mélangés dans un gobelet avant de se les injecter dans le pénis, puis l'avait mise enceinte». Elle me préciserait que «pendant cette partie de l'interrogatoire, ils avaient cessé de prendre des notes»: sans surprise, le compte rendu dont j'obtiendrai copie ne comporte aucune mention de 4chan. Néanmoins, vu le culot de Haefer et sa grande maîtrise du *lulz*, il est théoriquement possible, voire plausible, qu'une partie de l'entretien se soit bel et bien déroulée de cette façon. De plus, l'exclusion de cette citation est conforme à la méthodologie du FBI, qui (on le comprend aisément) n'a que faire du *lulz* (et cherche d'autant moins à le documenter). Selon deux autres documents qu'on me remettrait (dans lesquels sont relatés les interrogatoires, effectués le même jour, de deux Anons qui finiraient par être arrêtés), le genre consiste en un long résumé de l'interrogatoire émaillé par endroits de citations directes, résumé

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

se limitant aux éléments factuels sans s'attarder aux futilités. Le ton ou la dimension émotionnelle de l'entretien n'y sont nullement indiqués et ne font donc l'objet d'aucune analyse.

Et pourtant, à en juger par le récit des événements que m'a livré Haefer, ses petits gestes de défi en disaient long. Au cours de l'interrogatoire, comme on pouvait s'y attendre, les policiers et la jeune femme ont évalué les informations selon des critères très différents. Peu importe qu'ils aient été trollés ou non, et, s'ils l'étaient, qu'ils en aient été conscients ou qu'ils s'en soient offusqués (ou que j'aie moi-même été trollée), les agents ont rédigé un rapport qui s'en tient aux questions ayant une pertinence juridique[9]. «Haefer a alors demandé quel était l'objectif précis de la perquisition et de l'interrogatoire. L'agent spécial X a alors déclaré qu'il croyait qu'elle savait déjà pourquoi le FBI fouillait sa maison et l'interrogeait. Elle a répondu qu'ils étaient chez elle en raison "des attaques par saturation et du vandalisme"», lit-on dans le rapport.

Malgré cela, le document et le récit de Haefer concordent à maints égards. On lui a demandé plusieurs fois de «donner plus d'explications», ce à quoi elle a réagi en abordant toute une gamme de sujets, allant du rôle exact qu'elle avait joué dans les opérations à des réflexions plus larges sur l'éthique de l'attaque par saturation. Le rapport commence en indiquant qu'elle a affirmé «ne pas avoir tellement participé à l'un ou à l'autre [le vandalisme ou les attaques par saturation]», mais que, «après qu'on lui eut dit qu'elle n'était pas sincère» (d'après la preuve fournie par les journaux IRC, lui ont-ils dit), elle a admis avoir été pleinement consciente du fait que son ordinateur avait contribué à l'attaque contre PayPal et à la configuration de Low Orbit Ion Cannon (LOIC) sur d'autres machines. Elle leur a aussi donné tous ses noms d'utilisatrice, dont le rapport contient la liste, mais a prétendu ne pas se souvenir des noms des forums, de leurs administrateurs et de leurs serveurs en raison de leur trop grand nombre (dans d'autres comptes rendus auxquels j'ai eu accès, ceux et celles qui étaient interrogés éprouvaient moins de difficultés à s'en souvenir).

Le compte rendu d'interrogatoire de Haefer et les deux autres rapports que j'ai pu consulter font état – sans entrer dans les détails – des arguments

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

politiques justifiant les attaques par saturation. Mais Haefer m'a présenté cet aspect autrement: en m'indiquant qu'on lui avait posé des questions sur Assange. Rien de tel ne ressort du compte rendu, si ce n'est cette affirmation, par ailleurs digne d'intérêt: «Elle était d'accord avec l'idée de s'en prendre à PayPal parce qu'elle n'appréciait pas que PayPal bloque le compte de Julian Assange, retienne les sommes dues à Assange. Elle a précisé qu'elle n'était pas une fan d'Assange, qu'elle était simplement indignée par ce que PayPal avait fait.» Cet aspect s'ajoute à un résumé exhaustif de sa défense politique: «Haefer appuie les actions d'Anonymous. Quand un commerce ou une entreprise du monde réel a un comportement inacceptable, on peut manifester devant ses installations. Puisque Visa et MasterCard sont en ligne, on ne peut protester physiquement contre elles: on doit donc le faire en ligne ou mener une attaque par saturation. Pour Haefer, ces campagnes de protestation sont un "droit".»

Au cours de notre entretien, elle a précisé ce qu'elle entendait par «droit»:

> L'enjeu, c'était les droits. Il ne s'agissait pas de soutenir Assange. Il s'agissait de défendre la liberté d'expression, de réclamer plus de transparence de la part du gouvernement, de dire à ce dernier qu'il ne pouvait se mêler des affaires judiciaires d'autres pays, de lui rappeler qu'il travaille pour nous et non le contraire. Et, même si je n'aimais pas Assange, je croyais tout de même qu'il avait droit à la liberté d'expression et à un procès équitable. Et que, si l'on défendait seulement les droits des personnes qu'on aime, on ne défendrait plus des droits, mais des privilèges. Des privilèges, ça se supprime. Pas les droits. Ils ne peuvent qu'être bafoués.

Pour le FBI, se présenter chez les gens à six heures du matin relève de la procédure habituelle. Il en va de même des demandes de collaboration. La collaboration peut prendre différentes formes, allant de la divulgation d'informations sur place au consentement à devenir informateur. Haefer affirme qu'on a voulu la recruter (une requête qui figure également dans les

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

deux autres comptes rendus). Elle a refusé, ou, comme elle me le relaterait en des mots plus crus, «je les ai envoyé se faire foutre».

Après le départ des policiers, Haefer avait l'impression que, malgré tout ce qu'elle venait de leur dire, ils la considéraient encore comme une trolle sans scrupules plutôt que comme une militante. Avant de s'en aller, m'a-t-elle raconté, l'agent spécial lui a remis sa carte en lui demandant de «ne pas s'en prendre à sa famille. [...] S'il craignait encore cette possibilité, c'est qu'il ne comprenait toujours rien à l'affaire». Cela dit, nous ne connaissons pas sa version des faits: il pouvait tout aussi bien se laisser aller à un sarcasme...

En réfléchissant à ce qui lui est arrivé, Haefer, qui, comme tant d'Anons, a été prise au dépourvu par les agents fédéraux, en est venue à cette conclusion: «Si les policiers débarquaient à nouveau chez moi, je ne leur dirais probablement rien sur ce que j'ai fait.» Elle était tout de même fière – et l'est toujours – de sa modeste contribution à la défense des droits de la personne.

«Comment protester intelligemment»

À peu près à la même période, des dizaines d'autres personnes ont subi des interrogatoires similaires aux États-Unis. Quelques-unes ont partagé leurs histoires sur des forums peu de temps après, mais la plupart d'entre elles n'ont jamais eu la moindre idée de qui en est ressorti. Pendant ce temps, Anonymous a maintenu sa contribution à la pénible lutte pour le renversement d'un régime. Les Égyptiens sont descendus en masse sur la place Tahrir dans le cadre de la première d'une série d'occupations énergiques qui gagneraient également l'Espagne, puis l'Amérique du Nord et, enfin, d'autres pays d'Europe. Le 31 janvier, une masse de gens impressionnante, estimée à 250 000 personnes, a envahi la place. Mais l'enthousiasme et l'espoir ont été refroidis par l'escalade de la violence avec laquelle elle a été accueillie. Sur les canaux IRC, des Égyptiens ont demandé à Anonymous de s'en prendre au gouvernement et aux médias

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

contrôlés par l'État. Les Anons ont refusé. Même si certains d'entre eux menaient des attaques par saturation contre les sites web du gouvernement (au grand dam des membres de Telecomix), il régnait un consensus, dont les discussions sur IRC et les déclarations publiques se faisaient l'écho, selon lequel il était hors de question de s'en prendre à la presse (tous les pseudos ont été modifiés):

> <dr> salut, en tant qu'Égyptien, je vous implore d'attaquer leurs médias svp!!! http://www.ahram.org.eg/
> "http://www.algomhuria.net.eg/"
> http://www.algomhuria.net.eg/
> <MS> http://www.ahram.org.eg/ <-- le principal quotidien a seulement parlé du liban
> <sudor> les gars, faites-moi confiance, il serait beaucoup plus utile de bloquer ahram.org.eg
> <Fr> pas de médias
> <hat> sudor, j'ai défendu la même chose, mais c'est contraire à notre politique d'attaquer les médias, même s'ils appartiennent à un régime dictatorial
> <at> sudor, est-ce que les médias dont vous parlez font partie du gouvernement?
> <sudor> OUI!
> <tru> pas de médias
> <kan> les gars, l'Égypte vous adore et prie pour vous
> <Ter> PAS DE MÉDIAS
> <Cyberp> apprenez à pr073g3r la liberté d'expression
> <MS> ahram est un média mensonger
> <Ci> Tout comme le MCIT
> <cru> Merci, kanta
> <sudor> ahram appartient au gouv
> <Cyberp> les médias mensongers sont aussi des médias

Dans le cadre de leurs efforts, des membres d'AnonOps, de marblecake et de Telecomix ont édité une brochure incroyablement détaillée et illustrée

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

intitulée «Comment protester intelligemment».

À la fin du mois de janvier, AnonOps se comportait davantage comme un groupe de défense des droits de la personne que comme une bande de trolls assoiffés de *lulz.* Ses actions étaient de moins en moins unilatérales et de plus en plus axées sur le soutien au développement d'infrastructures pouvant permettre aux citoyens de contourner la censure et la surveillance électronique. Les Anons ont envoyé une «trousse d'aide» comprenant des outils de sécurité informatique, des conseils tactiques et des mots d'encouragement tel celui-ci, qui rappelle que les médias sociaux jouent un rôle limité dans de tels soulèvements, pourtant qualifiés de «révolution Twitter» par les commentateurs de tout poil: «C'est *votre* révolution. Elle n'aura pas lieu sur Twitter, à la télévision ou sur IRC. Vous *devez* prendre la rue, sans quoi vous *perdrez* la bataille.»

De nombreux Anons ont été ragaillardis par leur contribution au renversement de régimes dictatoriaux au Moyen-Orient. Pour d'autres, cependant, rien ne pouvait mieux démontrer l'emprise croissante de la *moralfaggotry* – les impératifs moraux – sur le collectif. En contribuant au Printemps arabe et à ses idéaux politiques, Anonymous a effectivement connu une transformation si marquée qu'on aurait dit que, à l'instar d'AnonSnapple, le *lulz* lui-même en avait été banni. Mais ce n'était pas le cas. Alors que des révolutions faisaient rage à l'autre bout du monde, une petite équipe de hackers prenait sa revanche contre un chercheur américain en sécurité informatique et sa firme. Le *lulz* faisait un retour en force.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Chapitre 7

La revanche du *lulz*

CERTAINES CARACTÉRISTIQUES FONDAMENTALES de la culture politique issue de l'anonymat n'ont rien de nouveau et ne sont guère difficiles à saisir. Prenons par exemple la fuite anonyme qui a fait connaître le Counter Intelligence Program (COINTELPRO), un programme illégal d'espionnage systématique de la population américaine. Par une nuit de 1971 en Pennsylvanie, des membres d'un groupe appelé Citizens' Commission to Investigate the FBI (commission d'enquête citoyenne sur le FBI) sont entrés par effraction dans un bureau local de la police fédérale à l'aide d'un pied-de-biche. Pendant que des millions d'Américains s'installaient devant leur télévision pour regarder Mohammed Ali en découdre avec Joe Frazier dans un match de boxe qui durerait 15 rounds, les activistes s'emparaient de plus d'un millier de documents. Ceux qui portaient sur la surveillance politique ont été transmis aux médias et publiés dans le numéro de mars 1972 du magazine *WIN*, le périodique de la War Resisters League (ligue des résistants à la guerre). C'est ainsi que le public a découvert l'existence du COINTELPRO. Mis en place en 1956 par le directeur du Federal Bureau of Investigation (FBI) J. Edgar Hoover, le programme est resté en vigueur jusqu'en 1971.

Au départ, le COINTELPRO visait un objectif bien précis: perturber le fonctionnement du Parti communiste des États-Unis, que Hoover croyait sous la coupe d'agents soviétiques. Très vite, toutefois, on a élargi sa portée aux mouvements politiques américains de toute sorte, dont des groupes de

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

gauche, de droite, même modérés. Un des buts avoués du programme consistait à «prévenir l'émergence d'un "messie" capable d'unifier et de galvaniser le mouvement nationaliste noir. Malcolm X était peut-être un tel "messie"; il est aujourd'hui le martyr du mouvement. Martin Luther King, Stokely Carmichael et Elijah Muhammed aspirent tous à jouer ce rôle. [...] King pourrait devenir un sérieux prétendant s'il renonçait à sa prétendue "adhésion" aux "doctrines progressistes des Blancs" (la non-violence) et souscrivait au nationalisme noir[1]».

Les documents rendus publics ont effectivement fourni une preuve tangible des démarches qu'avait entreprises le FBI pour surveiller King en particulier. Amorcée dès les années 1950, alors que Hoover venait tout juste d'autoriser le programme, la surveillance illégale du militant s'est poursuivie pendant plusieurs années. Lorsque King a prononcé son célèbre discours intitulé «I Have a Dream» à l'occasion de la marche sur Washington le 28 août 1963, le directeur adjoint du FBI William Cornelius Sullivan a écrit à Hoover: «Si ce n'est déjà fait, nous devons désigner King comme le Nègre le plus dangereux pour l'avenir du pays, du point de vue du communisme, des Nègres et de la sécurité nationale.» Le militant était décrit comme un «homme sans principes» affligé d'une «faiblesse de caractère». «Au moment opportun, quand cela pourra être fait sans nuire au Bureau, nous présenterons King comme un opportuniste immoral et hypocrite qui exploite la situation raciale dans son propre intérêt», poursuivait Sullivan. Peu après la consécration de King comme «homme de l'année» par le magazine *Time*, le FBI a obtenu l'autorisation illégale de mettre sa chambre d'hôtel sous écoute; «il y aura entrée par effraction», a-t-on écrit. La transcription des enregistrements a été remise à Hoover, qui a réagi en affirmant qu'elle allait «détruire le moricaud». En documentant l'infidélité conjugale de King, l'écoute électronique a soulevé l'enthousiasme du directeur et de son adjoint, qui pouvaient dès lors l'utiliser pour anéantir l'«animal»[2]. L'extrait d'une lettre du FBI envoyée à King pour le faire chanter a révélé une vérité historique disgracieuse, celle d'un gouvernement des États-Unis qui terrorisait un défenseur des droits civils parmi les plus vénérés et les plus pacifiques: «King, il ne vous reste

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

qu'une chose à faire. Vous savez laquelle. Vous disposez de trente-quatre jours (ce nombre a été choisi pour une raison précise, il a une signification concrète certaine). Vous êtes fini. Une seule porte de sortie s'offre à vous. Vous avez intérêt à la prendre avant que votre personnalité grossière, anormale et mystificatrice ne soit révélée à la nation[3].»

L'État s'en est pris de la sorte à de nombreux autres groupes: Students for a Democratic Society (SDS, étudiants pour une société démocratique), les suprémacistes blancs, des courants du mouvement féministe, le mouvement indépendantiste radical de Puerto Rico et d'innombrables associations opposées à la guerre du Vietnam. Entre autres méthodes brutales, le FBI ne se gênait pas pour user de manœuvres d'infiltration dans une perspective de sabotage: il cherchait ainsi à perturber systématiquement les mouvements politiques en vue de les éradiquer. Pour arriver à leurs fins, ses agents n'hésitaient pas à diffuser de fausses informations, à faire chanter des militants, à les traîner en justice pour quelque irrégularité fiscale, voire à recourir à la violence physique. Bénéficiant d'une marge de manœuvre démesurée, ils pouvaient alimenter les médias en nouvelles fabriquées et créer de toutes pièces des documents qu'ils attribuaient aux groupes visés. Certains des dommages les plus lourds étaient le fait de policiers infiltrés si profondément qu'ils parvenaient à éroder complètement les liens de confiance sur lesquels reposaient les mouvements. En vidant de toute leur vitalité des réservoirs abondants et légitimes d'activité politique, les agents du COINTELPRO alimentaient un climat de peur et de découragement.

Dans la foulée de la fuite orchestrée par la Citizens' Commission to Investigate the FBI, d'autres interventions ont eu lieu, dont la publication de documents du COINTELPRO obtenus par l'entremise d'une demande en vertu de la Freedom of Information Act, à partir desquels le journaliste de NBC Carl Stern a rédigé un article qui lui vaudrait un prix. Après que l'intimidation exercée pour affaiblir la dissidence politique légitime, légale et souvent modérée eut été révélée dans toute son ampleur, l'indignation était à son comble dans la population. En 1975, un petit groupe de sénateurs a mis sur pied la commission Church, dont l'enquête déboucherait sur une condamnation sans équivoque du programme: «Même si toutes les cibles

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

avaient eu recours à la violence, bon nombre des techniques employées seraient considérées comme intolérables dans une société démocratique, mais le COINTELPRO est allé encore plus loin. [...] Le FBI s'est comporté en *milice* perfectionnée[4].» (C'est moi qui souligne.) Un certain nombre de réformes suivraient, dont la limitation à dix ans du mandat du directeur du FBI.

Peu de temps après avoir subtilisé les dossiers de la police fédérale, la Citizens' Commission les avait fait parvenir à la presse avec un communiqué qu'elle voulait voir publié avec les articles portant sur l'affaire. Les militants y présentaient leurs motivations et leurs objectifs:

> Nous souhaitons diffuser ces documents le plus largement possible afin que tous les citoyens qui travaillent à rendre la société plus pacifique, plus juste et plus ouverte puissent les utiliser. Notre objectif ne consiste pas à mettre un terme aux violations les plus grossières de droits garantis par la Constitution qu'a commises le FBI dans le cadre de sa mission et de sa structure actuelles. Ni à attaquer personnellement des informateurs, des agents ou des administrateurs en particulier. Nous souhaitons plutôt contribuer au mouvement pour un changement fondamental et constructif de notre société, car, comme nous l'affirmions dans notre déclaration initiale, «tant que le pouvoir économique et politique restera concentré dans les mains de petites cliques à l'abri de tout contrôle et de toute surveillance, il faudra s'attendre à ce que la répression, l'intimidation et la provocation se perpétuent»[5].

Bien qu'ils eussent exprimé publiquement leurs intentions, les membres du groupe ont gardé l'anonymat jusqu'en janvier 2014, quand certains d'entre eux sont sortis de l'ombre[6]. Pour mettre au jour les méthodes malsaines du FBI, ces militants avaient agi dans l'illégalité; pour se protéger des conséquences de leur geste, ils avaient eu recours à l'anonymat. Leurs révélations spectaculaires n'avaient pas été faites en ligne; aucun d'eux n'avait porté de masque de Guy Fawkes, aucune fenêtre ne s'était affichée sur des écrans, aucun courriel n'avait été reproduit sur Pastebin et

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

WikiLeaks n'avait joué aucun rôle. Mais le concept était le même: il s'agissait de masquer son identité pour que l'attention ne se porte pas sur le messager, mais sur le message. Si la Citizens' Commission n'avait pas dérobé des documents rangés dans des classeurs et des tiroirs, peut-être le COINTELPRO se serait-il poursuivi en semant encore plus de désolation dans son sillage.

Faisons un saut jusqu'en 2011, au moment où Anonymous a rendu public un complot ourdi par une firme de sécurité informatique basée à Washington, HBGary Federal, dans le but d'espionner et de perturber WikiLeaks.

Vu la nature immatérielle des documents numériques d'aujourd'hui, il n'est plus nécessaire de quitter le confort de son foyer, et encore moins d'entrer par effraction dans un immeuble, pour mettre la main sur des dossiers secrets. En janvier 2011, donc, en se coordonnant sur Internet Relay Chat (IRC), des hackers d'Anonymous s'introduisent dans le système informatique de HBGary, d'où ils téléchargent 70 000 courriels de l'entreprise et d'autres fichiers, dont un diaporama PowerPoint intitulé «La menace WikiLeaks». Ce dernier document énumère des méthodes qui ressemblent à s'y méprendre à celles que les artisans du COINTELPRO avaient perfectionnées. On y met en avant un ensemble de tactiques qui, affirme-t-on, pourraient être «déployées dès demain»:

Palantir	Tactiques proactives potentielles

- Alimenter les conflits entre groupes. Désinformation. Créer des messages lors d'actions pour les saboter ou discréditer l'organisation d'opposants. Soumettre de faux documents puis dénoncer leur fausseté.
- Susciter des inquiétudes sur la sécurité de l'infrastructure. Inventer des histoires d'identités révélées. Si on croit que le processus n'est pas sûr, ils sont foutus.
- Mener des attaques informatiques contre l'infrastructure pour obtenir des données sur les fournisseurs de documents. Permet de tuer le projet dans l'œuf. Parce que les serveurs sont maintenant situés en Suède et en France, il est plus simple de rassembler une équipe pour y avoir accès.
- Lancer une campagne médiatique pour souligner la nature radicale et irresponsable des activités de WikiLeaks. Pression soutenue. Laisse les fanatiques indifférents, mais sème l'inquiétude et le doute chez les modérés.
- Chercher la source des fuites. Utiliser les médias sociaux pour établir le profil des employés et discerner les comportements à risque.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Les auteurs du diaporama proposent également d'identifier et d'intimider les donateurs de WikiLeaks et de salir la réputation de sympathisants et de journalistes tel Glenn Greenwald. Ces gens, explique-t-on, «sont des professionnels bien établis, de tendance progressiste, mais, à la longue, sous la pression, ils feront passer leur carrière avant la cause, car telle est la mentalité de la plupart des gens du milieu».

Bien qu'Anonymous ait illégalement porté atteinte aux serveurs de l'entreprise en volant ces documents, tout indique que les méthodes proposées dans le diaporama PowerPoint contreviendraient encore plus aux lois si elles étaient mises en œuvre. «Fabriquer et acheminer de faux documents dans l'intention de les voir publiés relève sans doute de la contrefaçon et de la fraude, explique Greenwald. Menacer les carrières de journalistes et de militants pour les faire taire constitue probablement une forme d'extorsion. [...] Attaquer l'infrastructure informatique de WikiLeaks en vue de nuire à ses donateurs enfreint indubitablement de nombreuses lois relatives aux réseaux numériques[7].»

Si la «menace WikiLeaks» est présentée dans un esprit très proche de celui qui animait COINTELPRO, les deux situations comportent un certain nombre de différences importantes. HBGary Federal n'est pas une agence de renseignement de l'État, mais une société privée ayant élaboré un plan pour des clients tout aussi privés. En partenariat avec deux autres firmes de sécurité, Palantir Technolgies et Berico Technologies, elle tente de convaincre le cabinet d'avocats Hunton & Williams, qui représente la Bank of America, du bien-fondé de sa proposition d'ébranler WikiLeaks. Travaillant de concert sous le nom d'équipe Thémis (qui évoque la déesse grecque de la justice et de l'ordre divin), Palantir et Berico espèrent que la présentation débouchera sur un contrat lucratif. Le 29 novembre 2010, en effet, Julian Assange a annoncé qu'il possédait des documents qui faisaient état d'un «écosystème de corruption» et «pourraient faire tomber une banque ou deux», et la Bank of America a des raisons de croire qu'elle pourrait être une de celles-ci. Selon le *New York Times*, les cadres supérieurs de la banque ont d'ailleurs entrepris de «passer au peigne fin des

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

milliers de documents au cas où ceux-ci seraient rendus publics» et ont retenu les services d'une firme de consultants et d'un cabinet d'avocats pour les «aider à gérer l'enquête[8]». La Bank of America n'a pas été nommée par Assange. En revanche, sa réaction, elle, a eu pour effet indésirable d'attirer l'attention.

Dans la foulée de la fuite des documents de HBGary, la Bank of America nie avoir été mise au courant de la proposition de l'équipe Thémis, qu'elle qualifie d'«abjecte», même si celle-ci était sans aucun doute destinée à un de ses groupes de juristes (Hunton & Williams ne commentera jamais l'affaire)[9]. En fin de compte, le plan de l'équipe Thémis ne sera pas appliqué, sans doute en raison de la fuite: comme il reposait sur des méthodes illégales, sa mise en œuvre n'aurait été envisageable que si ceux et celles impliqués avaient pu se protéger en niant son existence.

En plus de révéler des possibilités de perturbation directe, le contenu des courriels de HBGary a appris beaucoup de choses à Anonymous et aux autres groupes qui passent au crible les pratiques des entreprises en matière de sécurité. L'espionnage et le sabotage contre les travailleurs, les organismes à but non lucratif et les militants n'ont rien de nouveau. On se rappelle, par exemple, que pour intimider les ouvriers qui tentaient de se syndiquer, Henry Ford pouvait compter sur un service de sécurité interne dirigé par Harry Bennett. Ou que l'agence de sécurité Pinkerton, fondée en 1850 et toujours active aujourd'hui, a acquis sa notoriété en infiltrant les syndicats et en espionnant les travailleurs pour le compte de sa clientèle patronale. En fait, la pratique est à ce point répandue qu'elle a sa propre désignation: l'espionnage syndical. Plus récemment, la chaîne Walmart a été vivement critiquée après qu'on l'eut accusée d'avoir surveillé à grande échelle «ses actionnaires, ses critiques, ses fournisseurs, son conseil d'administration et ses employés[10]».

De nos jours, l'industrie privée de la surveillance est plus rentable, plus tentaculaire et plus solide que jamais. Elle se targue d'entretenir des liens avec les agences gouvernementales désignées par des sigles de trois lettres (bon nombre de ses membres comptent d'ailleurs des employés issus de ces agences ou des forces armées). Dans un rapport publié en 2013 et

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

intitulé *Spooky Business* (Une industrie qui donne froid dans le dos), le Center for Corporate Policy, une association ayant pour mission de surveiller les abus des milieux d'affaires, énumère plus de dix cas d'espionnage et d'infiltration par des entreprises (souvent pratiqués selon des méthodes dignes du COINTELPRO) contre des mouvements pacifistes et écologistes ainsi que des groupes militant, entre autres, pour la sécurité alimentaire, les droits des animaux et le contrôle des armes à feu. Greenpeace a d'ailleurs fait l'objet d'innombrables infiltrations: pour ne citer qu'un exemple, Électricité de France, qui avait mandaté une agence pour s'introduire dans les ordinateurs de la section française de l'organisme, a été condamnée à une amende de 1,5 million d'euros après que la tactique eut été rendue publique[11].

Le rapport saisit l'essence même du problème, troublant et actuel, des opérations d'infiltration auxquelles se livre le secteur privé: «L'espionnage privé a vu ses capacités exploser ces dernières années. [...] Employés, ex-employés ou sous-traitants actuels de l'État espionnent les associations à but non lucratif *sans être soumis à une réglementation et à une surveillance rigoureuses*, apparemment en toute impunité[12].»

Fournisseur de services spécialisés incluant des opérations d'espionnage «perfectionnées», HBGary est un acteur mineur de l'industrie. Néanmoins, après avoir passé au peigne fin les courriels divulgués par Anonymous et rédigé une dizaine de comptes rendus détaillés (qui seront ultérieurement compilés en un livre), une équipe de journalistes du webmagazine *Ars Technica* conclut que la menace d'une attaque contre WikiLeaks «n'avait rien d'une fanfaronnade». HBGary est à la fine pointe des services du genre. La firme a développé des logiciels de protection contre les programmes malveillants ainsi que des chevaux de Troie, des *rootkits** et des logiciels espions sur mesure, destinés à faciliter l'accès non autorisé à des systèmes informatiques. HBGary a aussi mis de côté un paquet de vulnérabilités jour zéro (ces vulnérabilités non encore divulguées) en vue d'un usage futur, s'assurant ainsi un accès direct à d'innombrables réseaux informatiques, ordinateurs et comptes de messagerie. Selon les documents ayant fait l'objet de la fuite, l'entreprise a fourni un dossier

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

contenant ces vulnérabilités, dont le nom de code est «Juicy Fruit», à la société Xetron, filiale du sous-traitant militaire Northrop Grumman[13].

Le public ignorait presque tout de ce marché des «jours zéro» jusqu'à ce qu'une série d'enquêtes journalistiques révèle son état florissant. Selon le *New York Times*, ces *exploits* se vendent de 35 000 à 160 000 dollars chacun. Ce sont les gouvernements qui paient les prix les plus élevés, s'assurant ainsi un contrôle non négligeable des vulnérabilités. Celui des États-Unis, en particulier, est considéré comme un client de premier ordre[14]. Les *exploits* peuvent être utilisés à des fins défensives, mais il est de plus en plus manifeste qu'ils servent souvent «d'armes offensives mises au service de toutes sortes d'activités, dont l'espionnage d'État, l'espionnage industriel et la fraude», constate le journaliste spécialisé Ryan Gallagher[15].

Bien qu'on en sache chaque jour un peu plus sur ces pratiques, la compréhension du sujet demeure incomplète et fragmentaire; les entreprises du secteur ont une mission plus vague que l'État et n'ont pas autant de comptes à rendre. La divulgation des courriels de HBGary et de HBGary Federal a permis de combler certaines lacunes en rappelant que «le travail est effectué en grande partie par le secteur privé, à l'abri de la surveillance des agences de l'État», conclut Nate Anderson[16].

Il importe de préciser que, contrairement à la Citizens' Commisson qui avait révélé l'existence du COINTELPRO, ceux qui ont mis au jour ces renseignements ne recherchaient rien de particulier. Le caractère accidentel de ces découvertes n'est pas exclusif à Anonymous. L'essentiel de ce qu'on sait de l'espionnage industriel a été «découvert par hasard, grâce à d'incroyables coups de chance», lit-on dans *Spooky Business*[17]. On pourrait cependant affirmer que ce bienfait pour la collectivité n'est pas un coup de chance, mais qu'il est plutôt attribuable à l'insatiable curiosité de hackers – même si ce sont les circonstances qui l'ont rendu possible. La divulgation des courriels de HBGary, par exemple, était l'œuvre de hackers assoiffés de vengeance.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

«Si nous sommes capables d'obtenir des informations à ce niveau, alors nous sommes une vraie CIA privée *lol*»

Mais revenons en 2011. Une semaine avant les attaques qui mèneront HBGary Federal à la ruine, le fondateur et PDG de HBGary, Greg Hoglund, fait l'éloge de son équipe dans une série de courriels. Il y transmet ses instructions au sujet de la surveillance d'un créateur de logiciels malveillants, puis conclut par une fanfaronnade:

> Ma chère équipe,
>
> Bon travail. Allez voir ce site, www.freelancesecurity.com et trouvez-y un enquêteur en mesure de surveiller et d'identifier formellement cet individu. J'en ai discuté avec Penny, qui m'a indiqué qu'elle *pourrait* accepter de vous aider à engager des ressources sur le terrain afin de garder l'œil sur la cible. J'aimerais avoir quelques photos de son lieu de travail, de son domicile, peut-être de quelques associés. L'adresse mentionnée ci-dessus est celle d'un site parmi quelques autres. Si nous sommes capables d'obtenir des informations à ce niveau, alors nous sommes une vraie CIA privée *lol*[18].

Hoglund veut donc faire de son entreprise un substitut aux forces de l'ordre et aux agences de renseignement, substitut qui soit plus incisif, plus redoutable et plus souple. Pourtant, dans les faits, HBGary développe surtout des solutions de protection contre les logiciels malveillants et les *rootkits*, ces programmes qui permettent d'avoir accès à des systèmes informatiques sans être détecté. Or, Aaron Barr, PDG de la filiale HBGary Federal, créée par HBGary dans le but d'obtenir de juteux contrats du gouvernement, souhaite se lancer dans la collecte de renseignements. Le titre prétentieux d'une conférence prévue pour la mi-février 2011 dans le cadre d'un forum populaire sur la sécurité à San Francisco (mais qui n'aura jamais lieu vu la tournure des événements) traduit cette ambition de façon manifeste: «Qui a besoin de la NSA à l'ère des médias sociaux?»

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Pour cette conférence, Barr a récupéré les données dont il a besoin en «infiltrant» Anonymous. Sous le pseudo de CogAnon, il a passé l'essentiel du mois de janvier à fréquenter les canaux IRC d'AnonOps et à mettre en corrélation l'activité qui s'y déroulait avec les médias sociaux. Dès que quelqu'un publiait un lien sur IRC, Barr se tournait vers Twitter pour vérifier si le même lien ou le même sujet y apparaissait simultanément, ce qui, le cas échéant, lui permettait de déduire que les pseudos employés sur l'une et l'autre plateforme se rapportaient à la même personne. En un mois, il a constitué une liste de pseudonymes, de noms véritables, de comptes Twitter et de lieux de résidence d'individus qui, affirme-t-il, sont les principaux acteurs d'Anonymous. Selon les courriels qui feront l'objet d'une fuite, Barr souhaite révéler leur identité et la transmettre au FBI en vue d'en tirer profit:

> De: Aaron Barr
> Sujet: Mise au point sur la conférence
> À: Mark Trynor, Ted Vera
> Date: Mercredi 19 janvier 2011 12:14:26-0500
>
> OK, je donnerai une conférence spéciale sur les médias sociaux @ BSIDES SF le mois prochain. Je compte avant tout y révéler l'identité des principaux acteurs du groupe Anonymous. Après tout, pas de secrets, non?:) Nous verrons jusqu'où j'irai. Je pourrais aussi parler un peu de la NSA, histoire d'avoir quelque chose à offrir à tous ces adorateurs débiles de la liberté d'expression. Oups, je viens de traiter de débiles les défenseurs de la liberté d'expression – ça me retourne l'estomac. Diable, je me retrouve dans une drôle de position.

Dans un autre courriel, Barr assure un collègue programmeur (qui a souvent mis en doute ses conclusions) que «je vais les vendre», en parlant des fiches d'identité qu'il a constituées[19]. (Le 5 février, les inquiétudes de ce programmeur auront pris une telle ampleur qu'il écrira un courriel contenant un avertissement prémonitoire: «Je crains que son arrogance soit

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

encore en train de prendre le dessus, ce qui s'est toujours mal terminé... pour chacun d'entre nous.»)

De son côté, le PDG considère que tout va bon train. Comment les Anons auront-ils donc vent de son infiltration? Chose incroyable, c'est Barr lui-même qui leur offrira l'information sur un plateau en rendant son opération publique. Le département des relations publiques de HBGary propose à Joseph Menn, du *Financial Times*, d'écrire un article sur la conférence à venir. Menn respecte «au plus haut point le travail de la filiale de HBGary», m'expliquera-t-il par la suite. «Parce que la structure et la traçabilité d'Anonymous sont des sujets d'un grand intérêt», il décide de publier le texte sans attendre. Le 4 février, les Anons se réveillent en lisant ces lignes: «Une enquête internationale sur les cyberactivistes qui ont attaqué les entreprises hostiles à WikiLeaks devrait mener sous peu à l'arrestation de membres influents du groupe ayant laissé des indices de leurs identités véritables sur Facebook et ailleurs sur internet, affirme-t-on.» L'article énumère des pseudos et émet des conjectures sur les lieux de résidence des participants, lesquelles s'avéreront fantaisistes:

> Un membre influent d'Anonymous, qui agit en ligne sous le pseudo d'Owen et vit manifestement à New York, semble être une des cibles des plus récentes enquêtes judiciaires, selon des communications en ligne divulguées par un chercheur indépendant en sécurité. [...] M. Barr a déclaré que Q et d'autres personnages éminents habitent en Californie, que la hiérarchie en place saute aux yeux, et que d'autres membres importants vivent au Royaume-Uni, en Allemagne, aux Pays-Bas, en Italie et en Autriche[20].

Owen et q (minuscule) sont certes des figures de premier plan d'Anonymous, mais le premier vit à Toledo, en Ohio, et le second habite en Europe.

Un article de fond dans une publication respectée constitue néanmoins un bien précieux pour toute entreprise. Si la société HBGary Federal se révèle assez teigneuse pour découvrir l'identité des gros bonnets d'Anonymous avant même le FBI, les cadres des grandes firmes se

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

bousculeront pour retenir ses services. Financièrement parlant, l'entreprise est au bord du gouffre, et un contrat avec Hunton & Williams viendrait changer la donne[21]. Dans leurs courriels internes, les dirigeants de HBGary parlent avec complaisance de l'avenir radieux qui, croient-ils, s'offre à eux:

> De: Greg Hoglund
> À: Aaron Barr Cc: Karen Burke, Penny Leavy, Ted Vera
> Objet: Re: Ça prend forme
>
> Nous devrions mettre ça à la une, poster des tweets. «HBGary Federal met la barre haut comme agence de renseignement privée.» Le jeu de mots avec *Barr* est voulu, *lol*. G.
>
> Le 2011-02-05, Aaron Barr a écrit:
> http://www.ft.com/cms/s/0/87dc140e-3099-11e0-9de3-00144feabdc0.html

L'entreprise n'aurait pu souhaiter attirer l'attention davantage – c'est pour le mieux, lui semble-t-il dans un premier temps. Le jour même de la publication de l'article, le FBI contacte HBGary Federal au sujet d'une réunion qui doit avoir lieu le lundi suivant à 11 heures. Cependant, comme le dira de façon mémorable l'humoriste Stephen Colbert, «Anonymous est un nid de guêpes, et Barr a affirmé: "Je vais me mettre le pénis là-dedans"». Après avoir lu le *Financial Times*, ces hackers, qui viennent tout juste de renforcer leur esprit d'équipe en attaquant des gouvernements du Maghreb et du Moyen-Orient, sont prêts à en découdre. Le texte donne les noms réels de nombreux Anons, et, vu les récentes vagues d'arrestations au Royaume-Uni et de perquisitions aux États-Unis, la situation est perçue comme urgente. Sabu est le premier à proposer de passer à l'attaque, mû en partie par son aversion profonde pour les hackers *white hats* et une industrie de la sécurité informatique qui, selon lui, fait commerce de remèdes de charlatan, à savoir de logiciels de sécurité déficients. Dans un premier temps, certains de ses camarades le suivent, mais pas tous. Plus tard, tflow racontera:

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> <tflow> au début, j'étais contre [son idée], je me disais que c'était une perte de temps et que ça alimenterait les trolls
> <tflow> mais quelques minutes plus tard, Sabu a découvert une vuln dans la sqli du site hbgaryfederal.com
> <biella> et la suite fait partie de l'histoire
> <tflow> ouais

Devant cette irrésistible vulnérabilité, toute l'équipe décide de monter à bord. L'encre du *Financial Times* est à peine sèche que les Anons s'insinuent déjà dans le système informatique de HBGary. Ils téléchargent des dizaines de courriels de la firme et de sa filiale, éliminent une multitude de fichiers avec leurs copies de sauvegarde et, prétendra-t-on, effacent les données du iPhone et du iPad de Barr. Un des premiers courriels sur lesquels ils tombent comprend un fichier PDF où figurent les données brutes recueillies par Barr à propos d'Anonymous. Ils y constatent rapidement d'innombrables erreurs. La plupart des personnes qui y sont nommées n'ont rien fait d'illégal, mais le défaut le plus flagrant du document est sans doute son ignorance des protagonistes de l'opération en cours, tels Topiary et tflow, pourtant connus du public et omniprésents sur les canaux IRC d'AnonOps, en particulier sur #reporter et #lounge.

À l'aide d'un logiciel de balayage conçu pour détecter les vulnérabilités connues, les hackers fouillent le site web de HBGary; très vite, ils en dénichent une qui touche son système de gestion de contenu. Dans son analyse en profondeur des détails techniques de l'attaque, le journaliste d'*Ars Technica* Peter Bright écrira: «En fait, [le système de HBGary] contenait un bug assez grossier[22].» En explorant le système, les Anons tombent aussi sur des mots de passe cryptés. La clé de chiffrement s'avère trop complexe pour qu'ils puissent eux-mêmes la craquer, mais, en ayant recours à la force brute d'un ensemble de processeurs graphiques, ils parviendront à décoder le tout en quelques heures.

Un des mots de passe, «kibafo33», donne accès au compte Gmail de Barr. C'est là que les Anons découvrent les échanges internes triomphalistes de HBGary. Instinctivement, ils testent ce mot de passe sur tous les comptes

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

de médias sociaux du PDG, ce qui leur permet de constater qu'il ne respecte pas la règle de base de la sécurité informatique: on ne doit jamais utiliser le même mot de passe d'une plateforme à l'autre. L'équipe peut maintenant prendre les commandes de tous les comptes de Barr, pour le *lulz* et pire encore. L'opération ne fait que commencer.

«Les bons drames doivent être drastiques[23]»

En ce dimanche du Super Bowl, le 6 février 2011, des millions d'Américains sont scotchés à leur écran pour regarder des gaillards se bousculer dans l'espoir de botter un ballon entre deux poteaux. Aaron Barr aurait pu faire partie du groupe, mais, quels qu'aient été ses plans, ceux-ci sont éclipsés par la violente opération de hacking dont il est en train de faire l'objet. Son compte Twitter piraté vomit les déclarations racistes et dégradantes les plus abjectes qu'il soit possible d'écrire en 140 caractères, accompagnées de son numéro de sécurité sociale et de son adresse personnelle. D'innombrables photos de lui, retouchées de manière peu flatteuse, circulent. Ses courriels, y compris des messages personnels regorgeant de détails embarrassants sur ses problèmes conjugaux, sont publiés sur The Pirate Bay.

Au cœur de la tourmente, Barr se connecte au serveur IRC d'AnonOps, où on l'invite à se rendre sur le canal dédié #ophbgary. Il accepte:

> <q> Eh, salut CogAnon
> <tflow> Bonjour M. Barr
> <Topiary> M. Barr et son infiltration d'Anonymous; «Maintenant, ils nous menacent directement», n'est-ce pas?
> <tflow> Je m'excuse par avance pour ce que vous et votre entreprise allez subir
> <q> Vous profitez du Superbowl, j'espère?
> [...]
> <tflow> Je suis vraiment désolé, M. Barr.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<tflow> Vous n'avez pas idée de ce qui reste à venir.
<Topiary> tflow, comment les choses avancent, justement?
<Topiary> CogAnon est vraiment un pro du 1337 [*leet*] avec sa capacité à faire des psyops en message privé dans la région de Washington
<CogAnon> ok, je me disais bien qu'il arriverait quelque chose comme ça
<Topiary> CogAnon, non, vous n'aimerez pas ce qui va se passer
<tflow> CogAnon, avez-vous une idée de ce qui va se passer?
<Topiary> Oh, une devinette rigolote!
<CogAnon> oh... t'as rien compris. c'était une recherche sur les vulnérabilités des médias sociaux... j'aurais jamais publié les noms
<Sabu> MENTEUR

Cette brève visite du dimanche 6 février n'aura été que le préambule à une discussion épique qui aura lieu plus tard, le même jour. La séance de chat qui suivra deviendra un des journaux IRC les plus consultés de l'histoire. Dans un internet dominé par des intérêts privés, l'IRC constitue une zone de liberté et d'autonomie. Quand des dizaines, voire des centaines de personnes se rassemblent en ayant la possibilité de dire ce qu'elles veulent et de prétendre être qui elles veulent, il est tout naturel que l'humour, l'esprit, la mise en scène et un certain chaos émergent. Si le monde est une scène (et que tous les geeks, hackers et sociétés de sécurité informatique ne sont que des acteurs), qu'en est-il d'internet? Une pièce dans la pièce, écrite en temps réel, à laquelle les acteurs contribuent une ligne à la fois? Chacun y fait ses sorties et ses entrées, mais rien n'en est connu à l'avance. Le résultat ressemble même à un scénario. La différence avec le théâtre réside dans sa dimension populaire, participative et improvisée, et dans la nature concrète de ses enjeux et de ses conséquences.

Acte I

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

La pièce que nous nous apprêtons à voir doit en partie son existence à Barrett Brown. Tard dimanche soir, le jeune Texan a apporté de bonnes nouvelles sur #ophbgary, un canal dont la finalité consiste à discuter de l'opération en cours et de la célébrer:

> <Laurelai> BarrettBrown, tu es là?
> <BarrettBrown> Je suis au téléphone avec le président de HBGary
> <Sneux> lol

Sabu fait une suggestion:

> <Sabu> BarrettBrown, demande à PENNY de venir ici et de parler.

À cette étape, il est de notoriété publique qu'Anonymous est en pleine campagne de hacking contre HBGary Federal et HBGary. La suggestion de Sabu est perçue comme une raillerie, et non comme une véritable invitation. Après tout ce qui vient de se produire, il est peu probable que Penny Leavy, présidente de HBGary, accepte de se jeter dans la fosse aux lions, dont les occupants sont qui plus est en train de réduire son entreprise en lambeaux. Mais c'est précisément ce qu'elle décide de faire. Sabu ouvre les hostilités en lui rappelant les faits embarrassants:

> <Sabu> penny. avant que nous ne commencions, sachez que nous avons tous [vu] les courriels échangés entre vous et les autres chez hbgary. alors ma première question est la suivante: comment avez-vous pu laisser aaron vendre de telles saletés au nom de votre entreprise?
> <ComradeBush> jesus cristo
> <Sabu> Penny, saviez-vous aussi qu'aaron colportait des informations fausses/fabriquées/bidon qui auraient pu mener à l'arrestation d'innocents?

Penny se porte à la défense d'Aaron Barr:

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<Penny> J'étais au courant de ses recherches sur les médias sociaux et le problème qui les caractérise, à savoir la facilité avec laquelle on peut prétendre être l'un des vôtres
<Penny> Il n'a jamais envisagé de les transmettre aux autorités. Jamais il n'aurait divulgué les noms, on ne parle que des pseudos
<Sabu> Penny, si ce que vous dites est vrai, alors pourquoi Aaron rencontre-t-il le FBI demain matin à 11 heures? SVP GARDEZ À L'ESPRIT QUE NOUS AVONS TOUS VOS COURRIELS.
<Sabu> alors penny comme je l'ai répété 4 fois nous avons tous les courriels. il y en a beaucoup où vous vantez les recherches d'aaron alors [...] je suis curieux
<heyguise> je suis encore en train de diffuser les courriels
<Penny> Je crois qu'il faisait quelque chose de bien, c'était informatif et ça soulevait plein d'enjeux liés aux médias sociaux

Rappelons que les courriels divulgués démontrent amplement l'intention de Barr de contacter les autorités en vue de leur vendre les données. Anonymous échafaude à la volée, sur IRC, une solution financière de son cru, une forme de chantage à la Robin des Bois:

<Sabu> penny. nous n'attaquerons pas hbgary.com. c'est déjà fait. ce que vous pouvez faire, c'est réorienter votre investissement de hbgaryfederal vers le fonds de défense de bradley manning. et prendre vos distances avec les recherches d'aaron barnetts (sic)
<Agamemnon> Penny [...], vous ne pouvez pas imaginer les attaques que nous subissons. Pas seulement de la police fédérale [...]: les combattants de droite pour la «liberté» essaient de nous éliminer [...], des agents infiltrés nous ont fait du tort [...], les recherches d'Aaron contiennent des renseignements personnels sur des gens qui n'ont rien fait d'autre que se présenter ici [...]. svp essayez de comprendre notre colère

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Pendant ce temps, au domicile de Brown, le téléphone sonne. Et c'est nul autre que Barr qui est au bout du fil. Les deux hommes discuteront en toute courtoisie pendant onze minutes (Brown enregistre la conversation, qu'il mettra en ligne par la suite). Un certain degré d'incertitude persiste quant à ce que HBGary entend faire des données recueillies. Barr, dont la voix ne trahit ni amertume, ni crainte, ni colère, se présente sur un ton confiant: «Je suis sous-traitant pour le fédéral, essentiellement dans le domaine de la sécurité.» Anticipant une question sur ses intentions, il déclare: «Je n'ai jamais envisagé de vendre les données au FBI.» Les courriels montrent pourtant qu'il a contacté la police fédérale dans le but d'en tirer profit d'une manière ou d'une autre, comme en colligeant ces noms mis en corrélation et en «révélant l'identité» des Anons, a-t-il lui-même écrit. On peut d'ailleurs présumer qu'un certain nombre d'organisations assiégées aimeraient bien connaître l'identité de leurs assaillants. Quelles qu'en soient les conséquences potentielles, les révélations contenues dans ces courriels sont perçues comme une menace inquiétante par l'ensemble des membres d'Anonymous.

À Brown, Barr offre une tout autre justification: il soutient que son objectif premier consiste à illustrer les failles des médias sociaux et à lever le voile sur la hiérarchie qui se cache derrière la ruche. «Il existe assurément une structure», affirme-t-il. Brown lui donne raison jusqu'à un certain point: «J'admets que quelques dizaines de personnes donnent le ton.» Mais il insiste sur le fait que beaucoup de noms sont erronés. «Je n'ai jamais prétendu que la liste était exacte à 100 %», insiste Barr, qui affirme avoir dit la même chose au *Financial Times.* «Le journaliste écrit ce qu'il veut.» Le PDG rappelle à Brown qu'il entend toujours rencontrer le FBI le lendemain matin, ajoutant que, dès lors, «l'affaire ne sera plus entre mes mains».

Les courriels indiquent que Barr et ses collègues se sont posé beaucoup de questions (jusqu'ici) sur la pertinence ou non de transmettre les noms au FBI. Ted Vera, président et directeur de l'exploitation de HBGary Federal, a conclu en défaveur de la divulgation: «Tu pourrais finir

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

par accuser la mauvaise personne. Ou alimenter la colère du groupe. Tu pourrais aussi t'être trompé, ce qui t'exploserait en pleine face, et dans la face de HBGary, au vu et au su du public. La seule possibilité que tu aies leurs noms véritables suffit. Inutile de les divulguer. Tu rencontres le FBI demain. Ça me surprendrait qu'ils partagent beaucoup d'information, mais il est possible qu'ils valident certains de tes résultats de manière officieuse ou par inadvertance.»

Anonymous, en revanche, n'éprouve pas de tels scrupules et publie le document en précisant à quel point Barr s'est fourvoyé en dressant sa liste de noms, pour la plupart erronés.

Comme il l'a fait avec Leavy, Brown tente d'attirer Barr en ligne. «Ils aimeraient que vous veniez. Je tenterai de maintenir un climat constructif», lance-t-il avec son accent du Texas. Ayant déjà goûté à cette médecine quelques heures plus tôt, le PDG résiste. Brown décide de changer de stratégie: «Je sais que vous vivez une journée difficile. On s'en est pris à vous. Je le répète: je n'ai rien à voir là-dedans, même si je ne condamne pas l'opération, car nous devons veiller sur nous-mêmes et sur nos intérêts.» La conversation téléphonique terminée, Brown ignore si Barr s'est laissé convaincre de prendre part à un second round.

De retour sur IRC, Brown, *gamer* passionné, annonce qu'il en a marre de «ces bêtises» et qu'il entend aller «jouer un peu à *Fallout: New Vegas*». Mais, avant de se déconnecter, à la demande répétée des Anons, il fait montre d'empathie envers Leavy:

> <Penny> Merci à tous, c'était un plaisir de discuter avec vous. Comment puis-je vous recontacter?
> <Sabu> penny, pouvez-vous demander à greg de venir devant votre ordi pour nous parler quelques minutes?
> <BarrettBrown> Si ça peut vous aider à vous sentir un peu mieux, sachez que je suis accro aux opiacés et que je suis encore sous traitement au Suboxone
> <BarettBrown> qui va prendre fin dans quelques jours
> <Penny> Hé Sabu merci d'avoir été si gentil, dure journée

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<Sabu> tout va bien. dure journée pour nous aussi

Acte II

Penny quitte la scène. Greg Hoglund la remplace au clavier de son ordinateur:

Penny répond maintenant au nom de greg
<evilworks> victoire
<q> victoire héroïque
<greg> Désolé les gars, c'était moi, c'était mon ordinateur et greg est parti
<greg> il est de retour
<Sabu> ok
<Sabu> GREG EST-CE QUE C'EST VOUS
<greg> ouais

Avant de poursuivre leur interrogatoire, les Anons prennent une pause pour se féliciter:

<'k> Greg, avez-vous déjà entendu parler des clés ssh? [une technologie de chiffrement]
<Sabu> en premier lieu, si vous ne l'avez pas encore lu, jetez un coup d'œil à http://pastie.org/1535735
<Sabu> c'est comme ça que nous avons mis la main sur rootkit.org
<evilworks> oh, génial Sabu
<q> joli coup
<q>:)
<q> toute une firme de sécurité
<Sabu> y a-t-il quelque chose que vous puissiez faire pour l'empêcher d'utiliser le nom de votre entreprise // hbgary?

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

La conversation s'interrompt un moment pendant que Greg consulte le journal de la fuite reproduit sur un *pastebin**. Il se rend vite compte de la gravité de la situation:

> <greg> alors vous avez le spool* de mon courriel
> <Sabu> oui greg
> <'k> greg nous avons tout
> <Agamemnon> Greg, je suis curieux de savoir si vous comprenez ce dont il est question. Comprenez-vous pourquoi nous faisons ce que nous sommes en train de faire?

«Nous avons tout.» À cette étape, si la pièce était jouée sur scène, Hoglund se lancerait sans doute dans un monologue pour se plaindre de son sort ou ferait à tout le moins quelque grimace d'effroi. Il a sans doute compris qu'il dispose de peu d'options. Néanmoins, si l'on ne peut duper les *tricksters*, on peut toujours les appeler à la raison... peut-être.

> <greg> vous rendez-vous compte que la diffusion de mon spool de courriel entraînera des millions de dollars de pertes pour HBGary?
> <c0s> greg, je crois vraiment que les gens qui sont ici sont sincères lorsqu'ils disent qu'ils préféreraient ne pas le rendre public. Mais leur décision reposera sur le sort que vous réserverez à Aaron.
> <c0s> c'est pourquoi je vous ai demandé de présenter ici vos idées sur ce qu'il est possible de faire
> <c0s> afin qu'ils sachent ce que vous pouvez faire
> <Sabu> greg, nous vous demandons essentiellement de prendre vos distances d'aaron, vous et votre entreprise
> <BarrettBrown> Comme je le disais, le moment est idéal pour un don à la Tunisie
> <evilworks> ou à Bradley Manning
> <evilworks> l'un ou l'autre

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Cet appel sincère portera-t-il ses fruits? La réapparition d'un autre personnage principal nous amène au dernier acte de la pièce.

Acte III

CogAnon fait son entrée:

> <Sabu> c'est aaron
> <Sabu> coganon
> <Sabu> c'est son PSEUDO D'ESPION
> <Sabu> salut aaron
> <c0s> Bonsoir, Aaron.

Hoglund prend le temps de se dissocier de Barr:

> <greg> aaron est le PDG de sa propre entreprise, qui, malheureusement, porte aussi le nom de HBGary, je ne peux rien faire sauf l'engueuler au téléphone
> <'k> hahaha ils sont tous là
> <greg> hbgary (mon hbgary) possède 15 % de hbgary federal, pour votre information
> <greg> ouais, et aaron n'a eu qu'à donner un petit coup sur le nid de guêpes n'est-ce pas
> <evilworks> je télécharge des courriels

Grâce aux courriels, on sait que, pour l'essentiel, les propos de Hoglund ne sont que du vent. Barr est un membre important et respecté de l'équipe de direction de HBGary:

> De: Greg Hoglund
> Date: Lundi 23 novembre 2009
> Objet: Bienvenue à Aaron Barr et à Ted Vera dans l'équipe de direction de HBGary

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

J’ai l’immense plaisir de vous annoncer qu’Aaron Barr et Ted Vera se joignent à l’équipe de HBGary! Ted et Aaron seront chargés de la gestion et de la direction de HBGary Federal, une filiale à part entière de HBGary qui se consacrera aux contrats de l’État. Tous deux possèdent une grande expérience et ont récemment mis sur pied une division de Northrop Grumman au chiffre d’affaires annuel de dix millions de dollars. Ils ont obtenu et dirigé des projets de développement de plusieurs millions de dollars et géré d’importantes équipes de travail. Nous connaissons Aaron et Ted depuis plus de cinq ans. Ces deux acteurs d’élite du milieu des sous-traitants du département de la Défense ont leurs entrées parmi cette clientèle. La semaine dernière, des acteurs très importants leur ont fait des propositions, mais tous deux ont choisi HBGary. C’est un très grand honneur pour notre entreprise. Les meilleurs attirent les meilleurs. Aaron occupera le poste de PDG de HBGary Federal et sera basé dans la région de Washington. Ted sera président et directeur de l’exploitation de HBGary Federal et travaillera à Colorado Springs. Bienvenue à bord!

Greg Hoglund, PDG, HBGary Inc.

Hoglund change aussitôt de tactique. Il fait appel à l’instinct de survie d’Anonymous:

<greg> vous rendez-vous compte qu'attaquer une entreprise américaine et voler des données privées, vous n'avez jamais fait ça?
<greg> je crois que vous auriez dû penser au risque que ça représente pour votre réputation
<Agamemnon> Greg. SVP répondez. Comprenez-vous bien qui nous sommes et pourquoi nous agissons comme nous le faisons?
<CogAnon> J'ai jamais pensé à vendre, vous vous trompez
<evilworks> nous nous FOUTONS de notre réputation

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<Sabu> greg, notre réputation n'est pas en jeu. la vôtre si.
<greg> vous avez mené une vraie opération de hacking, et je dois reconnaître que c'en était toute une
<evilworks> nous faisons ce que nous croyons juste
<c0s> Greg, les gens, ici, n'attachent aucune importance à la réputation
<evilworks> il existe de nombreuses façons de salir notre image
<evilworks> ça nous laisse indifférents
[...]
<Baas> Admettez que vous êtes incapables de foutre quelqu'un à la porte... Mais c'est l'intention qui compte. Nous voulons voir la réputation d'Aaron ruinée pour ça.
<evilworks> mon dieu!

Prenant une pause dans sa session de jeu vidéo, Brown fait un rappel:

<BarrettBrown> n'oubliez pas qu'il rencontre toujours le FBI demain à 11 heures
<c0s> c'est ce qui me dérange le plus
<Sabu> il a carrément sélectionné des gens au hasard sur facebook et les a associés à des pseudos d'irc
<BarrettBrown> et il va sans doute parler de moi

Malgré la colère qui se déchaîne autour de lui, Barr s'entête:

<evilworks> mais pourquoi avez-vous commencer à travailler là-dessus?
<BarrettBrown> Comme je le lui expliquais, ma famille s'est fait baiser par la police fédérale
<evilworks> c'était par intérêt personnel? pour une recherche?
<CogAnon> vous voulez que je réponde?
<Sabu> greg, répondez d'abord
<CogAnon> les gars, ça n'a plus d'importance, de toute façon [...] vous avez balancé mes courriels.
<evilworks> je crois que c'était pour le fric

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<Sabu> greg, svp répondez
<CogAnon> Je l'ai fait pour la recherche
<CogAnon> le fbi m'a contacté en raison de ma recherche
<CogAnon> dans le courriel où il était question de vendre des données, je parlais de vendre un modèle fondé sur ce type de recherche
<c0s> vous saviez, à moins d'être un parfait imbécile, vous SAVIEZ que vos méthodes avaient des défauts
<CogAnon> L'essentiel des données que j'allais présenter aurait pris la forme d'un organigramme des canaux IRC avec des icônes représentant les pseudos que je connaissais [...]
<evilworks> il nous reste des courriels à divulguer
<Sabu> aaron, vous nous devez des excuses, tout comme vous en devez aux investisseurs de hbgary, et vous devez rétablir les faits
<Sabu> en déclarant que vous N'AVEZ PAS établi l'identité de la direction d'anonymous
<Sneux> ^
<Sabu> et que votre recherche était purement théorique

Assommé, Barr en a assez:

<CogAnon> ok les gars, je vais me coucher. Je répète qu'il s'agissait simplement d'une recherche sur la vulnérabilité des médias sociaux [...] vous êtes allés trop loin, les mecs
<c0s> c'était la vengeance, œil pour œil dent pour dent, de gens à qui vous avez fait du mal
<Sabu> vous avez balancé l'identité de foutus innocents
<Sabu> allez vous faire foutre
<evilworks> allez vous faire foutre, ok?
<Sabu> regardez les noms sur votre docu
<Agamemnon> merde
<Baas> Le problème, c'est qu'il ne considère même pas qu'il a fait quelque chose de mal.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<Sabu> il est à l'aise avec la divulgation de données privées d'innocents
<Sabu> BORDEL DE MERDE
<Agamemnon> Greg, proposez-lui une entente [...] faites-le taire [...] et tout ira bien
<greg> une entente? quel genre d'entente?
<Agamemnon> Aaron se la ferme [...] vos courriels restent privés
<owen> les gars
<owen> contrôlez-vous
<CogAnon> c'était pour une recherche

Une pièce jouée sur internet a ceci de commode que personne ne sait ce qui va se produire et qu'on peut commenter comme on veut sans déranger personne. Tout le monde sait maintenant que je suis l'anthropologue en résidence. Un Anon m'envoie un message privé pour connaître mes réflexions sur l'épisode du moment:

<PKE> alors, c'est comment d'assister à tout ça?
<biella> salut PKE
<PKE> tu apprécies le spectacle?
<biella> pour l'essentiel
<biella> je suis un peu malade en ce moment, alors j'ai du mal à saisir tous les points de vue
<PKE> en tant qu'*outsider*, quelle est ton opinion jusqu'ici?
<biella> sur anonymous?
<PKE> euh, ça ratisse un peu large
<PKE> je parle de leur attaque sans merci contre hbgary et cie

J'avais eu du mal à suivre l'opération. Je souffrais d'une vilaine grippe, et je craignais qu'elle ne soit le signe avant-coureur de la rage. J'avais reçu ma dernière dose de vaccin quatre jours plus tôt, après une malencontreuse morsure de chauve-souris un mois auparavant. Malgré mes étourdissements, ma fièvre et ma gorge irritée, je répondis:

<biella> ça s'est fait très vite, ça m'a étonnée

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<biella> au début
<biella> puis la discussion sur le canal était tout à fait dans l'esprit du lulz
<biella> qu'on aurait cru relégué à l'arrière-plan au cours des opérations menées dans les semaines précédentes

Épargné par la grippe comme par les postulats irrationnels sur une éventuelle attaque de rage, PKE répliqua en se montrant plus incisif:

<PKE> absolument
<PKE> je veux dire
<PKE> un travail extraordinaire était accompli
<PKE> mais ça manquait vraiment de lulz
<biella> ouais, et maintenant on refait les stocks
<PKE> je crois qu'il s'agit plutôt d'un surplus
<biella> ha ha c'est vrai
<PKE> de mémoire récente, je ne me souviens pas d'une opération d'anonymous aussi ridicule
<biella> la discussion sur le canal avait quelque chose d'irréel
<biella> le fil twitter était monstrueusement scandaleux
<biella> ouais
<biella> vrai
<PKE> wow, j'avais jamais compris l'intérêt de la machine de haine d'internet avant ça
<PKE> quand tu mélanges des sociopathes et des altruistes enragés, t'as intérêt à te mettre à couvert

En fin de compte, insatisfaits de ce que les simples mortels avaient à offrir, les *tricksters* d'Anonymous décident de rendre publics les courriels de HBGary qu'ils gardaient sous la main en guise de levier de négociation. La semaine suivante, après que la plupart des messages eurent été diffusés au cours de la discussion sur IRC, Anonymous publie les 27 606 courriels de Greg Hoglund sur AnonLeaks[24].

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

La grosse tête

Pendant les jours qui suivent l'épreuve de force, le *lulz* bat son plein sur les canaux IRC, stimulant l'esprit du collectif. La presse est insatiable. Les journalistes cherchent à obtenir les commentaires de Barrett Brown, qui multiplie les interviews, de NPR à la BBC. Le 8 février 2011, c'est un Brown enchanté qui se connecte à #ophbgary:

> <BarrettBrown> NPR m'a demandé qui s'est occupé de HBGary
> <BarrettBrown> Je leur ai répondu «une équipe de ninjas d'Anonymous».
> <FEAR_Anonymous> NPR?
> <DingDong> HAHA
> <DingDong> oui!
> <FEAR_Anonymous> LOL
> <HateIRC> lol super
> <Sci> mdr

Vu de l'extérieur, Brown a tout d'un activiste d'Anonymous respecté et au sommet de sa forme. Vu de l'intérieur, toutefois, on n'a pas besoin de creuser bien loin pour constater qu'il suscite un certain mécontentement en raison du rôle qu'il s'est attribué avec un peu trop d'empressement. Les Anons s'enorgueillissent de rédiger collectivement leurs documents, dont la plupart portent sur les opérations. Or un peu plus tard en février cette année-là, apparaît un texte intitulé «Tout sur Barrett Brown. Allez-y de vos commentaires, les gars». Cette évaluation *de facto* du rendement du jeune Texan passe ses contributions au peigne fin (obtention d'aide juridique, rédaction d'éditoriaux, invitation de la presse sur IRC) tout en portant un jugement moral sur son comportement public. Notons que rien de tout cela ne se déroule à son insu. D'ailleurs, avant que ne soient publiés les commentaires critiques, on l'invite à rédiger une déclaration (citée en entier ci-dessous), qui sera reproduite au début du document:

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> Oui. Quiconque ignore ce que j'ai fait pour Anon n'a pas participé concrètement aux opérations Tunisie et Égypte, et quiconque n'a pas travaillé à l'actuelle campagne chaque putain de journée peut aller se faire foutre. Le plus dégueulasse, c'est que beaucoup plus de gens ont contribué à ce document qu'à n'importe quelle publication importante d'Anon. Voilà ma «déclaration», mes chéris. Veuillez aussi noter que la personne qui est derrière tout ça n'avait pas eu son paragraphe retenu pour le communiqué de presse, ce qui l'avait contrariée.
>
> Barrett Brown

Brown venant de dire à tout le monde d'aller se faire foutre, on comprendra aisément pourquoi les commentaires qui, sur sept pages, traitent de sa personnalité, de ses motivations et de sa contribution sont essentiellement négatifs. Ponctuées à l'occasion de commentaires positifs, les critiques condamnent unanimement sa tendance à l'autopromotion: «C'est important. Il est question des fondements de l'idéologie d'Anonymous que sont l'anonymat et l'égalité de tous.» «Tu sembles te croire assez exceptionnel et inestimable pour que les principes énoncés ci-dessous, l'anonymat et l'égalité de tous, ne s'appliquent pas à toi.» «Il n'est pas question ici de ton dévouement. Tu es sans doute un des plus importants amis des Anons. Je veux juste te dire que je ne veux de toi ni comme "chef d'Anonymous" ni comme porte-parole. Je sais que cela ne serait pas bénéfique pour Anonymous. +1 sincèrement +1 sans le moindre doute» «Anonymous va te soutenir dans la mesure où tu ne te constitues pas une armée personnelle et où tu t'abstiens de jouer les *leaderfags*. +1+1+1»

La petite équipe de hackers qui travaille dans l'ombre est également loin d'apprécier l'attention des médias reçue par Brown dans le cadre de l'opération HBGary. Un mois plus tard environ, Adrian Chen et John Cook publient un article dans *Gawker*, «Inside Anonymous' Secret War Room» (Au cœur du centre de commandement d'Anonymous), qui relate les suites de l'opération. Brown s'est longuement entretenu avec les journalistes:

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> Barrett Brown, considéré par la plupart des membres d'Anonymous comme le porte-parole du groupe, affirme qu'il était au courant de l'existence d'une «brèche de sécurité» depuis un certain temps déjà: «Nous connaissions la brèche de sécurité, car d'autres journaux d[u canal IRC] #HQ avaient été publiés auparavant (et je dois mentionner que #HQ n'est pas vraiment #HQ [pour *head quarter*, quartier général] – notez que ces journaux ne comportent aucune trace de la véritable coordination des opérations de hacking).»[25]

En lisant cet article, de nombreux Anons déjà irrités par Brown sont pris d'une rage folle. Ils le prennent violemment à partie sur #anonleaks, le canal dédié aux discussions sur les documents de HBGary publiés.

> <tflow> il est ironique de constater que tu prétends savoir exploiter les médias alors que tu n'es pas foutu de les informer correctement des faits essentiels.

Brown et Gregg Housh (c0s), qui communique aussi régulièrement avec la presse, reprochent aux journalistes leur propension à nommer un porte-parole même lorsqu'on leur explique qu'il n'y en a pas:

> <c0s> J'ai reçu deux coups de fil aujourd'hui. À la fin des interviews, les deux m'ont demandé
> <c0s> «pouvons-nous appeler votre porte-parole officiel»
> <BarrettBrown> allez, écoutez Housh
> <c0s> je dois me battre sans arrêt pour que ces abrutis ne le fassent pas
> <c0s> et certains acceptent de pas le faire
> <c0s> et comprennent très bien
> <c0s> mais leurs crétins de réviseurs les «corrigent»
> <c0s> et publient porte-parole ou une autre stupidité
> <BarrettBrown> et voilà
> <BarrettBrown> débattez avec Housh
> <c0s> ça fait chier d'avoir affaire à ces trous du cul

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<c0s> non
<c0s> je ne discute pas, hé
<tflow> alors vas-y et arrange-toi pour que les crétins de réviseurs corrigent le tout

Une fois cette question réglée, les Anons passent à d'autres aspects contrariants, notamment le fait que Brown prétende connaître de l'intérieur le canal #HQ, la brèche de sécurité de HBGary et le hacking, alors qu'il n'a même pas été témoin de l'opération, à laquelle il a encore moins contribué. Pire encore, il se trompe carrément à propos de #HQ, car c'est bien sur ce canal que l'opération HBGary a été coordonnée:

<'k> franchement, t'as même pas besoin de parler aux médias, t'as encore rien fait que t'as des explications pour tout
<BarrettBrown> ok, j'ai fait des trucs, mon chéri
<tflow> en plus, ça me fait trop chier que t'aies parlé de #hq à gawker
<FriedSquid> suggestion: être un journaleux, dans une certaine mesure, consiste à faire passer son message, à faire connaître son travail. À se faire connaître sous son nom.
<BarrettBrown> est-ce qu'on peut arrêter de parler de ça?
<tflow> alors que ça ne te concerne pas, c'est le moins qu'on puisse dire
<BarrettBrown> ils me l'ont demandé [...]
<tflow> alors tu fermes ta gueule et tu leur dis que ça te concerne pas si ça te concerne pas
<BarrettBrown> non, allez vous faire mettre zomg
<'k> c'est facile de dire «non» à un journaliste
<BarrettBrown> J'ai pas d'ordres à recevoir
<tflow> si tu sais pas de quoi tu parles

À l'instar de Snapple avant lui, Brown est chassé pour un temps du canal, cette fois par 'k. Suivent quelques commentaires finaux, dont certains

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

portent sur la qualité du spectacle, comme si la querelle avait rejoué à l'improviste une joute oratoire d'étudiants:

> <Earnest> j'aime pas prendre parti, mais 'k et tflow on été bien meilleurs que barrett sur ce coup-là
> <tflow> je l'aurais expulsé
> <tflow> mais j'aime pas expulser les gens
> <tflow> des séances de chats
> <'k> j'en ai vraiment ma claque de ces gigolos qui racolent les journalistes et disent n'avoir aucun rapport avec les opération tout en étant au courant de tout

Tandis que Brown fait face aux remontrances des Anons parce qu'il a essayé de se forger une renommée avec les opérations de hacking, HBGary rencontre une nouvelle série d'embûches et doit prendre des décisions difficiles.

Les suites

Le lendemain de sa séance de chat avec Anonymous et une semaine avant le premier congrès sur la sécurité informatique organisé par la société RSA Security, Greg Hoglund se plaint de sa situation à un journaliste: «Ils me causent beaucoup d'ennuis. [...] Ce qu'ils font, ce n'est pas du hacking militant, c'est du terrorisme. Ils ont franchi la limite[26].» L'accusation de terrorisme est inédite: jamais Hoglund ou Barr ne l'ont prononcée auparavant, que ce soit dans un courriel ou en public. Ce changement de discours est sans doute une tactique de relations publiques préparée avec soin: en les qualifiant de «terroristes», on présente ces hackers comme une grave menace à la société. Les dirigeants de HBGary font peut-être le pari de transformer en avantage la réalité embarrassante de la terrible (et potentiellement catastrophique) opération de hacking qu'ils ont subie. Hoglund décide aussi de ne plus participer au congrès de RSA.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Et effectivement: la société HBGary traverse certes une mauvaise passe, mais elle en sortira indemne, voire plus forte, entre autres parce qu'elle présente Anonymous comme une entité «terroriste» dont elle a été victime. Un an plus tard, un sous-traitant du secteur de la défense, Man Tech, se porte acquéreur de HBGary. Hoglund coopère étroitement avec les autorités dans leur enquête sur le collectif, comme le mentionne un communiqué de presse du FBI: «Les chefs d'accusation retenus contre six hackers, dont [Hector Xavier] Monsegur [dit Sabu], sont les résultats d'une vaste enquête. [...] Le FBI de Sacramento a minutieusement enquêté sur l'attaque menée contre HBGary et a transféré la cause à New York pour le procès de Monsegur. Chose importante, l'enquête de Sacramento a grandement bénéficié de la collaboration de HBGary elle-même[27].»

Aaron Barr et HBGary Federal connaissent un sort moins enviable. En tant que PDG, Barr ne peut pas être congédié, mais, en février 2011, il démissionne. Par la suite, l'entreprise fermera ses portes. Dans une interview qu'il accordera à Parmy Olson, du magazine *Forbes*, il reviendra sur les événements: «Est-ce que je regrette aujourd'hui [d'avoir fait ces affirmations]? Certainement. [...] J'ai reçu des menaces, et j'ai deux enfants. Deux enfants de quatre ans. Rien ne m'est plus précieux[28].»

Telle une Lady Macbeth lavant ses mains tachées de sang, Berico et Palanti, les deux autres membres de l'équipe Thémis qui ont comploté avec HBGary Federal en vue de discréditer WikiLeaks, rompent immédiatement leurs liens avec la firme et affirment ignorer les détails du plan. Mais, comme le souligne Nate Anderson dans *Ars Technica*, «les représentants de ces deux entreprises dans l'équipe Thémis étaient bien au fait de la proposition (ce qui n'était peut-être pas le cas de leurs patrons). Ils avaient vu les courriels de Barr et utilisé le fruit de son travail. Son idée d'attaquer WikiLeaks était reprise presque mot pour mot dans un diaporama de Palantir sur les "tactiques proactives"[29].»

Par la suite, un groupe de parlementaires démocrates ébranlés par leur découverte des tactiques proposées tente de lancer une enquête sur l'équipe Thémis. Dans une interview, le représentant Hank Johnson, qui dirige le comité, explique qu'une telle enquête est nécessaire parce que l'argent des

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

contribuables a servi à financer des outils et des programmes destinés à espionner des Américains au mépris de leurs droits garantis par le Premier Amendement[30]. Cependant, d'autres parlementaires, dont le représentant Lamar Smith, parviennent discrètement à empêcher la tenue de l'enquête. Les grands médias, hélas, restent indifférents à cette annulation.

Quant à Barrett Brown, l'insatisfaction des Anons à son égard ne lui coupe pas les ailes. Il reste actif au sein d'Anonymous pendant quelques mois. L'intrusion du collectif dans le secret d'une firme de sécurité privée comme HBGary Federal a motivé beaucoup de gens à contribuer bénévolement à un groupe de réflexion appelé Project PM (PPM), créé sur le web par Brown en 2010: «Nous devons porter notre regard au-delà des agences de renseignement qui nous ont systématiquement trompés par le passé, et surveiller leurs innombrables sous-traitants privés qui ont vu le jour ces derniers temps et sont appelées à nous tromper de façon encore plus efficace, selon une logique de marché[31].»

Tim Shorrock, un des rares journalistes d'enquête à se consacrer à la question, s'est penché avec intelligence sur la croissance galopante de cette industrie soumise aux forces du marché. L'information est clairsemée, explique-t-il, mais certains détails sont révélateurs de l'ampleur des opérations en jeu: «L'externalisation est devenue si omniprésente que le directeur du renseignement national a décidé d'étudier le phénomène l'an dernier. Mais une fois son rapport complété, en avril 2007, les résultats se sont avérés si renversants que le directeur a opposé son veto à sa publication et a déclaré à la presse que la divulgation des données qu'il contient constituerait un risque pour la sécurité nationale[32].»

Selon les chiffres actuels, on estime que le secteur privé accapare 70 % d'un budget américain du renseignement qui atteint 80 milliards de dollars[33]. Bien que les courriels de HBGary et de HBGary Federal n'aient pas permis d'avoir une idée de la taille de l'industrie dans son ensemble, ils ont tout de même offert un point de vue qualitatif sur l'ampleur colossale du monde de la sous-traitance en matière de renseignement. Avec des bénévoles qui le soutenaient dans la recherche, la rédaction et les tâches techniques, Brown a mis en place un dépôt centralisé dans le but de

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

cataloguer ce meilleur des mondes constitué d'entreprises spécialisées dans la collecte de renseignements, l'espionnage et l'infiltration pour le compte d'une clientèle tant privée qu'étatique. Si la divulgation des documents peut être qualifiée de percée, c'est parce qu'elle a donné un aperçu des stratégies employées par ces firmes privées à l'ère des réseaux numériques; il va sans dire que celles-ci n'hésitent jamais à proposer des manœuvres hasardeuses et à y prendre part. Barr, par exemple, s'apprêtait à fournir des renseignements exploitables en divulguant les données privées d'Anons qui n'avaient rien fait d'illégal (il a même transmis des pseudos et des lieux de résidence à un journaliste). Sa firme avait aussi élaboré un plan détaillé pour réduire à néant la carrière d'un journaliste. Parce que ces agissements sont désormais ceux de centaines d'entreprises privées, il est peu probable qu'une fuite unique de documents similaire à celle qui a révélé l'existence du COINTELPRO vienne mettre au jour le visage privé de l'espionnage. Le public devra plutôt se contenter de données fragmentaires du genre de celles que le hacking de HBGary a permis d'obtenir.

Inspirés par le succès de l'opération HBGary, d'autres Anons tenteront bientôt d'appliquer de semblables techniques à d'autres firmes de sécurité ou de renseignement. Dans un premier temps, toutefois, les hackers qui ont anéanti HBGary Federal quitteront AnonOps pour prendre part à une tournée de cinquante jours sous la houlette d'une troupe de théâtre expérimental appelée LulzSec. La critique des internautes sera dithyrambique. Mais les entreprises regarderont la pièce, qui enchaînera les rappels, avec effroi.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Chapitre 8

LulzSec

GROUPE DE HACKERS REBELLES doublés de ménestrels en rupture avec Anonymous, LulzSec est apparu quelques mois après l'infâme opération de hacking contre HBGary Federal. Constitué des gens mêmes qui, dans un esprit de vengeance, s'en étaient pris à Aaron Barr, LulzSec a entrepris, début mai 2011, une course folle, qui prit abruptement fin le 25 juin, peu après l'arrestation d'un de ses membres, Sabu, qui, en moins de vingt-quatre heures, retourna sa veste au profit du Federal Bureau of Investigation (FBI). Les cibles du groupe comprennent Sony Music Entertainment (Japon), Sony Pictures Entertainment, Sony BMG (Pays-Bas et Belgique), PBS, le ministère de la Sécurité publique de l'Arizona, le Sénat des États-Unis, la Serious Organised Crime Agency du Royaume-Uni, Bethesda Softworks, AOL et AT&T. Malgré une avalanche d'activités (et de nombreuses intrusions), le groupe était plus discipliné qu'Anonymous, du moins sur le plan organisationnel. Ses membres, qui pratiquaient le hacking en toute impunité, donnaient raison à l'affirmation de Fox News de 2007 selon laquelle Anonymous était composé de «hackers dopés aux stéroïdes».

Les membres de LulzSec jouaient leur rôle en sachant très bien que leur public était très divers. Même les hackers les plus arrogants qui, jusqu'ici, regardaient Anonymous de haut, soutenaient LulzSec. Des *black hats* de la vieille école vivaient les actions du groupe par procuration, émerveillés par son audace, son côté «tout est permis» et son désir

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

insatiable de dénoncer l'état pitoyable de la sécurité d'internet. La presse ne se lassait pas de ses facéties, dont elle peinait d'ailleurs à suivre le rythme. Avec ses innombrables intrusions et vols de données, LulzSec bousculait l'habituel cycle des nouvelles de trois jours. Pendant l'essentiel de son règne, le groupe narguerait les journalistes en leur faisant miroiter des informations, puis en gardant le silence – à une exception près: Parmy Olson, du magazine *Forbes*, s'est vu accorder la quasi-exclusivité (et pour conserver son privilège, elle s'est fait extrêmement discrète à propos de l'entente[1]).

Bien que LulzSec ait transmis suffisamment d'informations à Parmy Olson pour qu'elle puisse écrire ses articles, ses principales fenêtres sur le monde était son site web, son compte Twitter et le site Pastebin, où le groupe partageait toutes ses données et déclarations. En général, Pastebin est utilisé par les programmeurs pour publier des fragments de texte, du code source ou des conseils de configuration. Il génère une URL unique qui peut ensuite être collée n'importe où (sur Internet Relay Chat [IRC], par exemple) sous forme d'hyperlien. Ainsi, au lieu de coller des textes de plusieurs lignes sur un canal IRC (et d'en être chassé pour cause d'«inondation»), on n'a qu'à fournir un lien, qui prend normalement la forme d'une série de caractères aléatoires impossible à mémoriser et qu'on peut assortir d'une date d'expiration. Pastebin est un site parmi une multitude d'autres offrant ces fonctions, et la raison pour laquelle LulzSec l'a retenu reste un peu mystérieuse. Quoi qu'il en soit, il libérait le groupe de la nécessité d'entretenir une infrastructure pour ses communications. Quant au compte Twitter de LulzSec, il était très populaire, attirant parfois jusqu'à 20 000 nouveaux abonnés par semaine. Son *trickster* en résidence, Topiary, y rédigeait de croustillantes mises à jour qui revêtaient souvent une connotation maritime.

Pavillon pirate hissé haut, l'équipage de LulzSec voguait en haute mer, donc, loin en eaux internationales, et donnait son spectacle à qui voulait bien le regarder. Le *black hat* à la retraite David Mirza a noté:

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> Les membres de LulzSec débarquent sur internet armés d'une attitude *black hat* beaucoup plus redoutable que celle du collectif Anonymous d'où ils sont issus, une attitude dont l'authenticité saute aux yeux, avec tout le culot et le style nécessaires. Ils mettent la main sur des trucs, font du *doxing*, rendent justice. Personne ne peut leur mettre la main au collet, et ils le savent. Leur campagne est une grande saga devant laquelle certains hackers ayant déjà vécu une telle aventure se sentent à nouveau comme des adolescents[2].

En un seul tweet, le fanzine hacker *2600* a su résumer le sentiment général de la communauté geek: «Sites web hackés, infiltrations et scandales en entreprise, guerre par IRC, nouveaux groupes de hackers qui font la manchette... Les années 1990 sont de retour[3]!»

Aucune bande de pirates digne de ce nom ne pouvant se passer d'un vaisseau, l'équipage de LulzSec était à la barre du *Louise*. Ce nom était issu d'une erreur de lecture – et donc de prononciation – de «LulzSec» par un journaliste. Le navire étant pourvu de cabines infiniment spacieuses, on avait décidé d'embarquer une mascotte et, au lieu du classique perroquet pirate, on avait opté pour un pittoresque félin, un affable chat gris appelé Nyan Cat, bien connu des internautes pour son don d'embellir les ciels gris les plus mornes par un éternel arc-en-ciel lui sortant du cul. Cette joyeuse absurdité était tempérée par le porte-parole virtuel de LulzSec, qui lui tenait également lieu de logo: un bonhomme allumette arborant une vile moustache cirée à la française avec monocle, chapeau haut de forme et costume trois-pièces, un verre d'un excellent vin à la main. Ce gentleman on ne peut plus raffiné avait fait sa première apparition dans un *rage comic* (sorte de mème en bande dessinée très populaire chez les geeks) en langue espagnole avant d'être adopté par LulzSec en mars 2011. Considéré «comme un sir» par ses fans, ce personnage sans nom a fini par être appelé tout simplement «le sir». Tous ces éléments se sont conjugués pour doter LulzSec d'un imaginaire inédit pour les groupes de hackers de la nébuleuse Anonymous, imaginaire dans lequel se mêlaient profondeur, mystère et mythologie du mème. «Dès le départ, on aurait dit que LulzSec était déjà

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

nimbé d'une certaine mythologie pleinement développée, ce qui avait demandé des décennies à des groupes de hackers comme Cult of the Dead Cow», m'a expliqué un Anon ayant aussi été actif sur la scène *black hat.*

Mais revenons à la réalité un moment (nous explorerons les dimensions imaginaires un peu plus loin), et notons que ces hackers s'étaient regroupés sur leur propre canal IRC privé, à l'abri du drame dans lequel AnonOps était alors enlisé. Non liés par l'impératif catégorique de la *moralfaggotry*, ils menaient leurs opérations de hacking contre toute cible jugée pertinente, quelles qu'en soient les raisons, fussent-elles farfelues.

On peut être étonné d'apprendre que LulzSec a surgi, déjà mûr, d'une banale discussion sur IRC. On l'est moins lorsqu'on sait que ces hackers en avaient un peu marre d'Anonymous, et que certains d'entre eux s'étaient peu à peu lassés de participer à des opérations organisées par d'autres. Or, que font des *tricksters* mis au repos? Tout ce qu'ils peuvent pour chasser l'ennui. Il faut reconnaître que le fait qu'ils aient été en possession d'un stock de données subtilisées à Fox News qui n'attendaient que d'être divulguées, et qu'AnonOps ait été plongé dans un désarroi croissant a aidé.

L'Enfer n'a pas de fureur qui égale celle d'un *gamer* dédaigné

Pendant l'essentiel de mars et avril 2011, donc, AnonOps poursuit ses activités sans relâche, mais le réseau se bute à une accumulation de problèmes. De petits incendies éclatent çà et là, et la fatigue résultant de leur extinction commence à tirer le groupe vers le bas.

Même si, en se faisant crucifier par Anonymous, Aaron Barr est devenu *la* risée d'internet pour l'année 2011, sa mission consistant à découvrir et à révéler l'identité des Anons n'a pas pris fin avec lui. La société Backtrace Security (dont le nom se veut un clin d'œil à la tristement célèbre campagne de trollage menée en 2010 par Anonymous contre la pré-adolescente Jessi Slaughter, dont le père avait affirmé avoir «retracé» [*backtraced*] les Anons) en a fait son principal objectif et a repris le travail là où Barr l'a laissé en plan. Sa représentante la plus active, Jennifer Emick,

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

a elle-même déjà combattu l'Église de scientologie aux côtés d'Anonymous dans le cadre de l'opération Chanology. Elle a cependant fini par se montrer critique à l'égard des tactiques discutables adoptées ultérieurement par AnonOps (celles-là mêmes dont LulzSec garnirait son coffre à outils). Défenderesse autoproclamée de la loi et de l'ordre, elle soutient que «personne ne peut prétendre se battre pour la justice et la démocratie tout en appliquant des tactiques injustes et antidémocratiques[4]». L'argument est pertinent, mais passe sous silence l'éthique douteuse de sa propre conception du travail de justicier: à la mi-mars 2011, Backtrace publie un tableau indiquant l'«identité» de 70 membres et sympathisants d'Anonymous. Comme dans le cas de la tentative de Barr, beaucoup de ces identifications sont soit erronées, soit déjà publiques, à l'exception d'une seule. On doit l'accorder à Backtrace. Il s'agit du nom qui compte alors le plus: Hector Xavier Monsegur, hacker notoire connu sous le pseudo de Sabu. (Dans le document de l'entreprise, son patronyme est mal orthographié: Montsegur.)

Backtrace n'a pas découvert l'identité de Sabu en accomplissant quelque prouesse ingénieuse. La firme a simplement eu de la chance: une membre d'Anonymous, qui fréquentait les canaux les plus secrets du collectif sous le pseudo de Laurelai, a sottement transmis ses journaux de chat à Emick. Dans ce document totalisant plus de 200 pages se trouvait un indice qui a mené Backtrace au New-Yorkais d'origine portoricaine établi dans le Lower East Side de Manhattan. En chattant avec ses compatriotes, Sabu avait accidentellement tapé ou collé une adresse web comprenant le nom de domaine de son serveur personnel, prvt.org. En googlant cette adresse, l'équipe de Backtrace a découvert un sous-domaine recelant des renseignements personnels sur le hacker, ce qui l'a inévitablement mené vers sa page Facebook.

Intitulé *Namshub* («incantation» en sumérien), le document de Backtrace est disséqué par Anonymous, mais la plupart des Anons sont bien sûr en mesure de savoir si les pseudos correspondent bel et bien aux noms réels. Sabu (et peut-être quelques-uns de ses proches collègues hackers de longue date) se sait exposé. En divulguant l'identité de l'Anon, Backtrace a

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

agi tel la force d'Eshu: l'esprit des chemins a laissé choir le puissant hacker au carrefour. En effet, démasqué, Sabu-Monsegur a une importante décision à prendre. Voyant son nom sur la liste, il pourrait effacer tout le contenu de son ordinateur, entrer dans la clandestinité et, au bout de quelques années, revenir en héros. Cependant, il ne peut pas le faire tout de suite: cela indiquerait de manière «flagrante que son identité a été révélée» (m'expliquera ultérieurement tflow). ll pourrait ainsi revenir un mois après l'expiration du délai de prescription, pour retourner tranquillement sur son *isla del encanto* chérie (Puerto Rico) en toute sécurité et y raconter ses exploits à ses proches. En son absence, la renommée de ce hacker plus grand que nature, déjà considéré comme une légende, ne ferait que s'accroître. En rester là serait par conséquent la meilleure chose à faire. Mais Sabu ne manque pas d'orgueil.

Il décide plutôt de contacter Emick, qu'il bombarde de fausses informations afin de semer la confusion. Selon un de ses camarades hackers, «quand les gens de Backtrace ont publié leur tableau de noms, [Sabu] a tenté de leur faire croire qu'il était un agent double travaillant pour un fournisseur d'accès internet en vue d'infiltrer Anon, mais ils ne l'ont pas cru».

Bien connu de ses semblables, Sabu faisait au contraire profil bas en public. Du moins, avant de voir son identité révélée. Peu de temps après cela, il publie un premier tweet: «Salut! On me connaît sous le nom de Sabu ces jours-ci. J'ai créé ce compte pour tirer certaines choses au clair, en particulier en raison des révélations de #backtraceinsecurity.»

Convaincu d'être intouchable, Sabu continuera de jouer les *tricksters* plus ostensiblement que jamais, jusqu'à ce que son rôle d'indic soit révélé au grand jour un an plus tard. (À sa sortie de prison, Sabu sera devenu un fléau pour Anonymous. Le jour où il sera démasqué, un de ses compatriotes ayant déjà été un de ses collègues hackers déclarera sans retenue sur IRC: «Mieux vaut passer cinq-cents ans en prison que de se regarder dans le miroir en sachant qu'on est une ordure.»)

J'ai demandé à quelques hackers comment ils réagissaient aux tentatives de *doxing* comme *Namshub*. Un des rares membres importants de

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

LulzSec (qui, à ce qu'on en sache, n'a jamais été identifié ou arrêté) m'a transmis un exposé en quatre points qui résume bien le sentiment que j'ai perçu chez les autres:

> <Avunit> A) Vous avez confiance dans le fait que les autres se protégeront suffisamment pour que ça reste sans impact
> <Avunit> Tout va bien et vous voulez qu'on se serre les coudes, parce que ça marche
> <Avunit> Vous ne vous en faites pas avec les noms
> <Avunit> Ça pourrait être le mauvais nom, n'est-ce pas?

Le 1er avril 2011, peu après la publication par Backtrace des saletés de *Namshub*, AnonOps lance l'opération Sony. «Préparez-vous à l'assaut le plus terrible que vous n'aurez jamais vu, dans le plus pur style Anonymous», annonce une vidéo[5]. L'opération commence par une mégacampagne d'attaques par saturation contre le réseau PlayStation de Sony (PSN), qui perturbe le service et les *gamers* qui l'utilisent. Pour comprendre pourquoi AnonOps s'en prend à cette cible, il faut remonter à janvier 2011, alors que Sony intentait une poursuite judiciaire contre le turbulent (et précoce) hacker américain George Hotz, mieux connu sous son pseudo geohandle. Ce dernier s'était spécialisé dans le «débridage», une technique qui consiste à libérer des appareils destinés au grand public, comme les iPhone et les consoles de jeu, de la mainmise de leur fabricant afin de les rendre configurables selon les désirs de leur propriétaire. Habituellement, la tâche requiert une analyse approfondie de l'appareil en question, la mise au point d'un logiciel capable d'en désactiver les contrôles d'accès et de copie, et la publication d'instructions permettant à d'autres personnes d'en faire autant. Cette forme de hacking a pour but de convertir une machine spécialisée en un ordinateur d'utilité générale, jugé préférable. Bien qu'un appareil à fonction unique soit utile aux personnes qui ne veulent pas se casser la tête, de nombreux spécialistes de la technologie estiment qu'une telle contrainte constitue une restriction arbitraire de leur droit d'utiliser ce qui leur appartient comme bon leur semble. Ils

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

considèrent également le débridage comme un défi stimulant, un peu comme si le fabricant avait créé un puzzle spécialement pour eux.

C'est en 2007, à l'âge de 17 ans, que Hotz a reçu ses premières louanges de la part de hackers et de militants pour les droits numériques en devenant le premier hacker à déverrouiller un iPhone. Puis, en 2009, il s'est attaqué à la populaire console PlayStation 3 (PS3). Avec une équipe d'anonymes appelée fail0verflow (aucun lien avec Anonymous), il a réussi à débrider le système en cinq semaines seulement. Le 26 janvier 2011, il répandait la bonne nouvelle en publiant les instructions de débridage de la PS3 sur son site web, ce qui n'a pas manqué d'attirer l'attention sur lui. Une fois débridée, une console permet d'effectuer des tâches impossibles avec une PS3 ordinaire: jouer à des jeux piratés, faire des copies de sauvegarde, jouer à des jeux directement à partir du disque dur (ce qui raccourcit considérablement le délai de chargement), lire des vidéos, installer GNU/Linux et, sans doute le plus important, créer, innover et apprendre d'une multitude de façons. Interviewé à propos de sa prouesse par la BBC, Hotz a paraphrasé une devise classique des hackers: «[La PS3] est censée être impossible à hacker, mais rien n'est impossible à hacker.»

Les entreprises ont évidemment leurs propres devises, dont une pourrait aller ainsi: «Vous hackez, nous poursuivons.» Peu après que Hotz eut publié ses instructions de débridage, Sony l'a poursuivi en justice pour violation du droit d'auteur et infraction à la Computer Fraud and Abuse Act (CFAA). Connu pour son franc-parler, le jeune homme n'est pas resté les bras croisés. Il a parlé haut et fort. En fait, techniquement, il a rappé sa réplique (depuis sa publication sur YouTube, elle a été visionnée plus de deux millions de fois). Sur la vidéo, on peut le voir, assis dans un fauteuil de sa chambre ordinaire et vêtu d'un sweatshirt élimé: «Yo, c'est geohot, et pour ceux qui l'savent pas, j'suis poursuivi par Sony.» Il marque le *beat* en secouant ses boucles enfantines tandis qu'il traite les gens de Sony d'«enculeurs». Son rap se conclut ainsi: «Mais bordel / c'est qu'une compagnie / et je personnifie / la liberté pour tous[6].»

La poursuite civile intentée par Sony ne visait pas seulement Hotz et plusieurs autres hackers, mais aussi une centaine de «M. ou Mme Untel»,

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

dont certains étaient soupçonnés de faire partie de l'équipe anonyme du jeune homme. La multinationale est même allée jusqu'à pister les internautes qui avaient simplement consulté les instructions de débridage. Le tribunal lui a permis d'exiger du fournisseur d'accès internet de Hotz les adresses IP des personnes ayant été sur son site de 2009 à 2011, et YouTube s'est vu demander de transmettre des renseignements sur celles qui avaient visionné la vidéo sur le débridage ou l'avaient commentée. De nombreux geeks ont été consternés par la poursuite, un sentiment qu'a bien saisi l'auteur de science-fiction et militant pour un internet libre Cory Doctorow, selon qui il est «absurde et injuste pour une multinationale gargantuesque d'utiliser ses ressources juridiques colossales pour écraser un hacker solitaire dont le seul "crime" est d'avoir cherché le moyen de faire des trucs (légaux) avec un objet lui appartenant de plein droit[7]».

L'affaire a semé l'émoi dans les rangs d'Anonymous. Le fait que Hotz n'ait jamais demandé l'aide du collectif (avec lequel il n'a en fait jamais voulu se mêler) était sans importance.

Ainsi, le 2 avril 2011, Anonymous publie une première déclaration:

> Chers ~~enculés cupides~~ SONY,
>
> Félicitations! Vous avez réussi à attirer l'attention d'Anonymous. Vos récentes poursuites judiciaires contre nos concitoyens internautes geohot et Graf Chokolo ont été perçues comme une attaque impardonnable contre la liberté d'expression et la liberté d'internet, sources premières du *lulz* libre (et vous savez ce que le *lulz* représente pour nous). Ce faisant, vous avez porté atteinte à la vie privée de milliers d'innocents qui ne cherchaient qu'à faire circuler les informations librement. En supprimant ces informations, vous avez obéi à votre cupidité d'entreprise et à votre désir de contrôle total sur les faits et gestes de ceux qui achètent et utilisent vos produits, du moins quand ces gestes menacent de nuire à la mainmise corrompue que vous cherchez à conserver sur ce «droit» d'auteur tordu (*copywrong*[8]*).*

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Très vite, l'opération dégénère. En menant une attaque par saturation contre le PSN, Anonymous ne se fait pas de nouveaux amis: le collectif soulève plutôt la colère des *gamers*, qui, privés de leur distraction favorite, écument de rage. Dans le feu de l'action, un groupe dissident appelé SonyRecon se forme en vue de divulguer des données privées appartenant aux cadres de Sony. L'initiative suscite la controverse parmi les activistes d'Anonymous et dans leur réseau de sympathisants.

Devant le mécontentement provoqué par l'opération, Anonymous se ravise et publie une nouvelle déclaration: «Nous avons réalisé que prendre le PSN pour cible n'était pas une bonne idée. Nous avons donc décidé d'interrompre l'opération jusqu'à ce que nous trouvions un moyen d'agir sans nuire à la clientèle de Sony.» Les Anons espèrent ainsi pouvoir éteindre l'incendie.

Au cours du mois d'avril, toutefois, le PSN continue de subir des interruptions. Et puisque c'est Anonymous qui a, au départ, lancé l'opération, bon nombre d'observateurs imputent ces problèmes récurrents à la horde d'activistes masqués. Mais une poignée d'individus isolés annonce en être responsables et Anonymous finit par affirmer sans ambiguïté: «Pour une fois, ce n'est pas nous.»

Durant ces longues semaines, en l'absence de toute déclaration officielle de la part de Sony, les rumeurs et les insinuations vont bon train. Finalement, le 26 avril, la multinationale publie un communiqué: «Nous avons découvert que, du 17 au 19 avril 2011, certaines données de profils d'utilisateurs ont été compromises en raison d'une intrusion illégale et non autorisée dans notre réseau[9].» Des millions de numéros de carte de crédit auraient été dérobés, ce qui amène Sony à inviter ses clients à modifier leurs mots de passe et à rester à l'affût de tout signe de fraude. La situation ne fait que s'aggraver lorsqu'on annonce que le PSN demeurera inaccessible pendant un certain temps. *Gamer* passionné, le professeur Colin Milburn écrira un compte rendu captivant de cette infâme opération de hacking du point de vue des utilisateurs lésés du PSN: «À cette étape, l'émotion s'est muée en indignation, en grande partie à l'égard de Sony

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

pour son laxisme en matière de sécurité, mais surtout à l'endroit des hackers ayant perpétré l'intrusion[10].» En fin de compte, l'interruption durera vingt-quatre pénibles journées[11].

Fin mai, Sony affirme que l'opération lui a fait perdre 171 millions de dollars[12]. Bien que la multinationale ne fournisse aucune preuve de cette perte financière, les événements ont été pour elle un véritable fiasco dont les coûts se calculent non seulement en argent, mais aussi en temps et en réputation. Appelés à témoigner devant le Congrès des États-Unis, ses cadres sont réprimandés pour leur laxisme en matière de sécurité et leur manque d'empressement à avertir leur clientèle. Au Royaume-Uni, Sony sera condamnée à 250 000 livres sterling d'amende par le bureau du commissaire à l'information, qui imputera catégoriquement la faute à l'entreprise: «Quand on est responsable d'une telle quantité de données bancaires et de comptes utilisateur, la sécurité des données doit être une priorité absolue. Dans l'affaire qui nous occupe, ce n'était précisément pas le cas; quand la base de données a été prise pour cible (même si l'attaque était résolument criminelle), les mesures de sécurité en place étaient nettement insuffisantes[13].»

Dans la tourmente, les cadres de Sony tentent de jeter le blâme sur Anonymous, prétendant avoir trouvé sur le serveur de leur société un fichier incriminant le groupe. Mais jamais un hacker d'Anonymous ou de LulzSec n'admettra avoir commis le crime ni ne sera mis en accusation (cinq d'entre eux, avec deux associés, verront leurs disques durs confisqués pour analyse judiciaire et seront jugés coupables de dizaines de crimes de hacking). Encore aujourd'hui, le mystère du hacking du PSN reste entier.

> «Blanchiment d'argent, versement de bitcoins, fraudes d'assurance-versement, réseaux de zombies, fuites de données»

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

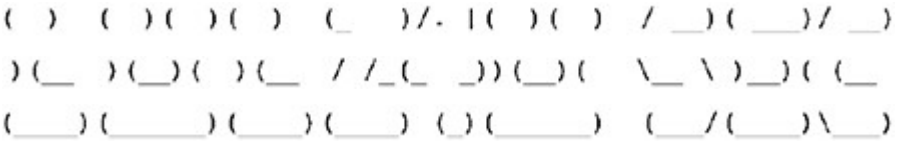
Les malheurs subis par le PSN dans la foulée de l'opération Sony ont créé un contexte favorable à l'émergence de LulzSec. À la mi-avril, des hackers fréquentant #internetfeds parviennent à se frayer un chemin dans les serveurs de fox.com, où ils volent une base de données commerciale. Outre des renseignements personnels sur des journalistes et d'autres employés de Fox, celle-ci contient plus de 70 000 adresses courriel et mots de passe associés à des téléspectateurs qui se sont inscrits au site pour être tenus au courant des auditions pour l'adaptation américaine de *The X Factor*, un télé-crochet dont la diffusion débutera sous peu. Les données subtilisées permettent aussi aux Anons de prendre le contrôle de certains comptes Twitter de Fox News. Fox n'ayant commis aucune ignominie récemment (à part continuer d'exister), les hackers sont conscients de se trouver dans une situation délicate. Divulguer des renseignements personnels ou des données sur l'entreprise au nom d'Anonymous leur attirerait sans doute un torrent d'invectives de la part des Anons de la base, qui les pressent d'ailleurs de réfléchir à des solutions alternatives. Le cadet du sous-groupe, tflow, a déjà une suggestion à faire, laquelle s'inspire vaguement de Goatse Security, la «firme» de trollage et de sécurité de weev qui, en 2010, a divulgué des données dans le but de couvrir de honte le géant des télécoms AT&T:

> <tflow> On devrait créer un concurrent à Goatse Security
> <tflow> qui hackerait pour le lulz
> <tflow> Lulz4u Security[14]
> <pwnsauce> LOL oui
> <pwnsauce> tflow est-ce que t'as le journal (log) d'hier soir??
> <tflow> lequel?
> <pwnsauce> Il faut qu'on retrouve l'interface système
> <pwnsauce> d'après toi
> <tflow> demande à X
> <pwnsauce> je crois qu'il se sert de son téléphone pour ça

Pour en arriver au nom de «LulzSec», tflow y va d'un classique intemporel d'internet, l'art ASCII:

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<tflow>: 
<tflow> «On l'a fait pour le lulz» ~LulzSec
<pwnsauce> MAGNIFIK
<pwnsauce> t'as fait une page de défaçage?
<pwnsauce> en fait, je pensais à aujourd'hui
<Palladium> haha
<tflow> LulzSec, la division lulz des InternetFeds
<Palladium> je préfère les opérations de hacking politiques
<tflow> ouais
<tflow> mais
<tflow> qu'est-ce qu'on pourrait faire avec fox.com?
<tflow> à part le défacer pour le lulz?
<tflow> y a rien de politique là-dedans
<tflow> c'est pas comme quand on a défacé pm.gov.tn
<pwnsauce> lol

Pour une raison que j'ignore, la proposition de tflow n'a pas abouti pas tout de suite. Quand je l'interrogeai plus tard sur les causes de cette indifférence, il m'a dit ne plus s'en souvenir. Peut-être n'y avait-il pas assez de monde en ligne pour faire un consensus, ou peut-être les Anons connectés à IRC étaient-ils distraits par d'autres activités. Les discussions sur IRC sont parfois difficiles à expliquer, même au moment où elles se déroulent, et il vaut mieux ne pas trop y chercher de raisonnement causal après coup. Je ne m'y risquerai donc pas, du moins pas dans le cas qui nous occupe. Ce qui est certain, c'est que tflow prend momentanément congé d'Anonymous à la suite d'une dispute avec un opérateur caractériel qui menaçait d'attaquer le réseau AnonOps. Et tflow n'est pas seul. D'autres Anons quittent temporairement les canaux pour n'y revenir que le 4 mai:

<Sabu> le charmant tflow est de retour
<Falcon> bonne nouvelle

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<tflow> quoi de neuf?
<Falcon> pas mal de trucs, tflow, heureux de te voir de retour
<pwnsauce> YOUPPI
<Falcon> ici Topiary en passant
<Sabu>;p
<Sabu> bonne nouvelle, tflow est de retour

À nouveau réunis et très heureux de l'être – en fait, ces Anons ne le seraient-ils pas encore plus s'ils avaient une raison de divulguer les données de Fox? Car la pression pour ne pas diffuser les données au nom du collectif leur semble désormais encore plus forte qu'avant: la débâcle de Sony leur a bien fait comprendre qu'une opération de hacking aléatoire pouvait susciter la colère des membres d'Anonymous. Ils envisagent un moment de les publier sur 4chan «sous anonymous avec une minuscule», comme le suggère tflow. Sabu propose de transmettre l'information à la journaliste de *Forbes* Parmy Olson, dans l'espoir «de la motiver à écrire son livre». (Les auteurs dont je suis savent que rien ne vaut une fuite colossale de données d'entreprise, avec mots de passe et courriels etc., pour se mettre dans de bonnes dispositions d'écriture. Si seulement ils *m*'avaient transmis les données, ce livre aurait paru un an plus tôt!) Mais aucune de ces idées ne l'emporte. Finalement, Topiary, qui, ces dernières semaines, est resté silencieux sur AnonOps, mais a été actif sur les canaux secrets, se connecte à IRC sous le pseudo de Falcon. Alors que Sabu suggère de confier les données à Olson, Topiary propose de les diffuser par le compte Twitter LulzLeaks:

<Falcon>: Attendez, on devrait les diffuser sur @LulzLeaks
<Falcon> notre twitter

tflow relance le nom de LulzSec, qui n'avait pas été retenu jusque-là, et cette fois avec un peu plus d'insistance:

<tflow> à mon avis on devrait créer une pseudo-marque lulzsec
<tflow> genre
<Sabu> aussi, que quelqu'un contacte parmy

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<tflow> Lulz4u Security
<Sabu> lui dire qu'on a une nouvelle fuite pour elle
<Sabu> en exclu
<tflow> Goatse Security
<pwnsauce> OUI
<pwnsauce> tflow – j'aime ça
<Falcon> Parmy dort
<Sabu> réveille-la
<Sabu> hahaha
<Sabu> pensez à un nom cool les gars
<Sabu> vite
<tflow> Lulz4u Security?

Sabu est impatient:

<Sabu> alors
<Sabu> pourquoi on fait pas ça simplement sous la bannière anonleaks
<Sabu>?
<tflow> parce que [...]
<pwnsauce> J'aime bien LulzLeaks et Lulz4u Security

D'autres participants manifestent leur opposition à l'idée de Sabu en rappelant la distinction entre fuites éthiques et non éthiques:

<tflow> anonleaks, c'est pour les fuites éthiques
<lol>:D
<tflow>:P
<Falcon> http://twitter.com/#!/LulzLeaks
<lol> nan:D
<lol> c'est important?
<Falcon> LulzLeaks!
<lol> le hacking et les fuites de données sont jamais éthiques xD
<pwnsauce> on a le twitter LulzLeaks xD
<Falcon> voilà ce qu'on devrait faire:

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<Falcon> – télécharger la base de donnée
<Falcon> – la diffuser sur LulzLeaks
<Falcon> – la retweeter à partir des comptes officiels de Fox News

Après quelques autres suggestions de noms, dont Ninjasec, les hackers finissent par s'entendre sur LulzSec. Une fois le nom choisi, ils peuvent commencer à discuter de la divulgation et des supports visuels:

<Sabu> Lulz Security / lulzsec
<Falcon> comme image, je verrais bien Batman en train de baiser un requin
<Falcon> mais celle-là, elle est déjà grillée
<Sabu> lol
<Sabu> on s'en tient à celles-là pour une semaine ou deux
<Sabu> et on attire l'attention sur la fuite x factor
<Sabu> après, on malmène les gestionnaires/vendeurs de fox
<Sabu> puis on embarrasse le fbi avec infragard
<Falcon> quelqu'un fait connaître @lulzsec partout
<Falcon> les nouvelles, /b/, partout où on peut le diffuser
<Falcon> AnonOps

Quand on a quelque chose de tout neuf, c'est une bonne idée de préparer une présentation:

<tflow> rédiger une déclaration?
<Falcon> Pas sûr de ce qu'on peut écrire... hum
<Falcon> J'imagine qu'on pourrait se présenter
<Falcon> en tant que LulzSec

En trois minutes, Topiary pond une déclaration. Puis, il fête l'événement aux... cookies.

<Falcon> Salut, bonjour, comment allez-vous? Splendide! Nous sommes LulzSec, une petite équipe d'amoureux du lulz affligée de

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

voir la monotonie de la cybercommunauté étouffer l'essentiel: le plaisir. Considérant que le plaisir est désormais réservé aux vendredis, les vendredis où l'on attend le week-end avec impatience, nous avons pris l'initiative d'étendre le plaisir, le plaisir, le plaisir, du plaisir sur l'année entière. En guise d'introduction, vous trouverez...
<Falcon> ...ci-dessous les coordonnées des concurrents à The X Factor 2011. D'autres informations suivront et si vous nous aimez et que vous aimez voir des gens se mettre en colère, suivez-nous sur twitter! twitter.com/LulsSec
<tflow> parfait
<Falcon> mais c'est @LulzSec
<Falcon> Merde, j'ai écrit ça en 2 mn, je reviens je m'attrape un cookie

Topiary et Sabu pressentent ce qui va se passer:

<Sabu> oh les mecs lol
<Sabu> on va bien s'amuser
<Falcon> LulzSec à son meilleur
<Falcon> Blanchiment d'argent, versement de bitcoins, fraudes d'assurance-versement, réseaux de zombies, fuites de données
<Falcon> c'est parti pour le lulz

Mais cet accès d'enthousiasme n'aboutit à rien. La première fuite de données est accueillie avec indifférence par la presse. LulzSec est totalement inconnu, et la divulgation a eu lieu un vendredi, une très mauvaise journée pour envoyer quelque chose aux médias. Protégés par leur nouvelle bannière, les hackers décident donc de se focaliser sur un potin juteux concernant un opérateur d'AnonOps, Ryan Cleary, qui vient de se retourner contre le collectif.

À ce moment-là, Cleary, qui coordonne un vaste réseau de machines zombies, est un opérateur d'AnonOps à la fois des plus impopulaires et des plus puissants. (À maintes reprises, d'ailleurs, j'aurai vent de plaintes à

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

propos de comportements erratiques de sa part, tel que chasser des participants de canaux privés et publics plus ou moins arbitrairement.) Peu après la création de LulzSec, le bruit court que Cleary a mené une attaque par saturation contre le réseau AnonOps. Il aurait aussi divulgué les noms de plus de 600 utilisateurs d'IRC avec leurs adresses IP. (AnonOps a pour politique de ne pas conserver les adresses IP des utilisateurs lorsqu'ils se déconnectent, mais, en cours de session, les opérateurs ont accès à toutes celles qui ne sont pas masquées par un réseau privé virtuel [VPN].) Pourquoi Cleary aurait-il agi ainsi? Ayant vécu de nombreux conflits avec d'autres opérateurs, il aurait décidé de prendre sa revanche. Aussi, selon un de ses collègues d'Anonymous, il tente d'impressionner Hack the Planet (HTP), un groupe de hackers marginaux disant posséder «une longue et impressionnante liste de trucs». Ses membres n'apprécient guère Anonymous, comme en fait foi la dernière phrase de l'ultime numéro de leur fanzine (particulièrement actif en 2011, HTP tirera sa révérence en 2013): «Buvons aux deux années de HTP, les amis! N'oubliez pas de prendre ça cool, de vous marrer, d'être les meilleurs et de tirer à vue sur Anonymous[15].»

Pour se la jouer auprès de hackers underground qui ne peuvent pas voir Anonymous en peinture, quoi de mieux que de sacrifier des Anons, dont quelques potes? (Plus tard, Cleary se rétractera. Selon tflow, il «était jaloux de LulzSec, où il rêvait d'être admis, ce qui explique pourquoi il nous a offert son réseau de zombies».) Les guerres intestines entre hackers sont depuis longtemps un atout précieux pour les enquêtes policières. Sans surprise, en réaction à la crasse de Cleary, un sympathisant d'Anonymous lui rend la monnaie de sa pièce en le doxant à son tour. Personne n'a la certitude que le nom balancé est bien le sien, mais, comme dans le cas de Sabu, il s'avérera que oui. LulzSec est mentionné noir sur blanc dans le bulletin de HTP, ce qui pousse ses membres à revenir sur les derniers événements:

<Sabu> mais on doit anéantir ryan
<Sabu> il a nui gravement à anonymous avec ça

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<Falcon> ou quelque chose
<lol> en tout cas, on a ses coordonnées maintenant
<Falcon> il a une voix agaçante

Rendus furieux par le geste de Cleary, les autres opérateurs d'AnonOps publient une déclaration où ils présentent leurs excuses aux membres d'Anonymous et les invitent à se tenir loin du réseau pour un moment, le temps pour eux d'améliorer la sécurité du système. Avec cette pause sont réunies les conditions parfaites pour que LulzSec soit catapulté sous le feu des projecteurs.

LulzSec à proprement parler

LulzSec prend la mer à la barre d'un cargo chargé des données subtilisées à Fox, d'un compte Twitter tout neuf et de mèmes internet en abondance, comme en témoigne la justification fournie par ses membres lorsqu'ils finissent par publier lesdites données: «Savez-vous qui nous défendons? Allons donc. Fox l'a qualifié de "rappeur abominable"; nous qualifions Fox de vulgaire racaille. Vous croyez que nous avons fini? La partie de plaisir ne fait que commencer[16].» Chaque membre de l'équipage est déjà habitué au rythme et aux excentricités des autres. Ces Anons sont devenus si proches que tous connaissent leurs lieux de résidence approximatifs (bien qu'ils ne se disent jamais leurs vrais noms). La plupart sont basés au Royaume-Uni ou autour, à l'exception de Sabu. Certains ont même commis l'imprudence de communiquer par Skype, ce qui explique pourquoi Topiary a pu qualifier la voix de Cleary d'«agaçante».

La sécurité opérationnelle, souvent désignée par l'apocope anglaise «OpSec», est l'art d'assurer la protection des interactions humaines et numériques au sein d'un groupe. La vigilance quant au niveau de sécurité d'un ordinateur et d'un réseau fait partie de ses fondements. Le fait de dépendre de logiciels propriétaires (dont on ignore le code source et les pratiques commerciales du fabricant) peut entraver cette vigilance. L'utilisation de logiciels libres tel GNU/Linux et le non-usage d'outils

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

comme Skype (réputé pour ses portes dérobées à l'usage des autorités) sont des mesures essentielles à l'optimisation, jamais achevée, de la sécurité opérationnelle. La protection des données privées en est un autre pilier. Un individu qui transmet volontairement de telles informations n'a pas à se préoccuper du niveau de sécurité de ses logiciels et de ses appareils, mais toutes ces considérations – et bien d'autres encore – doivent être prises en compte en amont de la moindre opération de hacking, qui, autrement, équivaut carrément à une demande d'arrestation. Tout ça pour dire que, en règle générale, la sécurité opérationnelle ne fait pas partie des points forts de LulzSec. D'ailleurs, dans la foulée de la série d'arrestations qui frappera ses membres, les pratiques du groupe seront érigées en modèle de ce que tout bon hacker militant *ne doit pas* faire.

Mais, pour le moment, de telles inquiétudes sont loin à l'horizon, et la mer semble vaste, pour ne pas dire infinie. Au cours des six semaines qui suivront, LulzSec accomplira des exploits remarquables. On pourrait penser que je parle ici de l'inventivité technique du groupe, mais, à quelques exceptions près, ses opérations se démarqueront plutôt par leur audace et leur style que par leur sophistication informatique.

LulzSec parviendra à susciter une prise de conscience et à générer un débat sur un ensemble d'enjeux allant de l'état pitoyable de la sécurité d'internet à l'appétit insatiable des médias pour le sensationnalisme. Ce sera là son apport le plus important.

«Pourquoi nous aimons secrètement LulzSec» (pas si secrètement, en fait)

Les hackers ne voient pas tous Anonymous d'un bon œil. Sur le plan technique, les interventions du collectif sont souvent trop rudimentaires pour gagner le respect des gens du métier. Certains hackers ont l'impression que ses stratégies nuisent à la cause de la liberté sur internet, tandis que d'autres trouvent ses mauvais tours puérils. Il en est également pour qui l'activisme de perturbation, si pertinent soit-il, n'est simplement pas leur

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

truc. Avec LulzSec, c'est une tout autre histoire. Un nombre étonnant de hackers, en particulier dans le domaine de la sécurité informatique, tombent sous le charme du nouveau groupe ou lui vouent à tout le moins un respect ambigu. Afin d'expliquer les raisons de cet engouement, laissez-moi vous donner un aperçu de cette sous-culture en vous racontant comment j'y ai été introduite.

Avant l'apparition de LulzSec, j'ai fait connaissance avec le milieu new-yorkais de la sécurité informatique essentiellement par la force des choses. Apparemment, j'avais contrarié des hackers spécialisés en sécurité lorsque j'avais fait l'éloge, par écrit, des développeurs de logiciels *open source* (ces programmeurs qui distribuent leur code source sous licence ouverte) en les qualifiant de hackers. S'étant sentis rabaissés par mon «erreur», des chercheurs en sécurité, se qualifiant également de hackers, m'avaient fait part de leurs réactions de diverses façons: suggestions constructives, invitations à débattre, mais aussi railleries et menaces. Ils voulaient me montrer qui étaient les «vrais» hackers – à savoir eux-mêmes. Vous croyez qu'un grille-pain télécommandé qu'on met en marche grâce à un ordinateur à code source ouvert appelé Raspberry Pi relève du hacking? Non, désolé. Vous pensez la même chose de la programmation des *throwies* à DEL clignotantes que vous souhaitez distribuer lors d'une rave? Non plus. La conception de ces gadgets aussi cools qu'utiles – et invariablement clignotants – exige certes un certain savoir-faire technique, mais ce n'est pas du hacking. Le hacking, m'expliqueraient ces experts, implique une entrée par effraction numérique: on s'insinue dans un système, on en prend le contrôle et on en fait ce qu'on veut. Je venais de publier mon essai sur les «hackers» du logiciel libre, intitulé *Coding Freedom: The Ethics and Aesthetics of Hacking*, et ces gardiens du vocable de la sécurité informatique semblaient avoir trouvé ma conception du terme trop étroite, car j'avais omis d'y inclure leur univers. Elle est pourtant beaucoup plus nuancée qu'ils ne le pensaient. Et si ma définition du hacking englobe les programmeurs de logiciels libres, les bidouilleurs qui fabriquent des bidules *et* les informaticiens qui s'introduisent dans des systèmes; cela ne signifie

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

pas qu'il faille parler de tout le monde en même temps. Mon premier livre traitait d'un sujet bien circonscrit.

Du reste, chacun de ces micromilieux revendique le titre de «hacker» et conteste la prétention des autres à s'en réclamer. Je n'ai donc guère été étonnée quand le monde de la sécurité informatique s'est écrié que celui du logiciel libre n'était pas fait de «hackers». Et j'ai tout de même apprécié les discussions constructives que nous avons eues – beaucoup plus que les menaces voilées.

Quelque part en 2010, j'ai reçu un courriel d'un hacker respecté qui m'encourageait à assister au NYSEC, le rendez-vous informel des professionnels new-yorkais de la sécurité informatique qui a lieu tous les mois dans un bar. Sur Twitter, l'événement est décrit comme «une rencontre, autour d'un verre, avec un problème de sécurité de l'information». Pourquoi pas? me suis-je dit. Il s'agissait là d'une façon cordiale de me dire: *viens voir la réalité, commence à fréquenter de vrais hackers*. D'autres de mes interlocuteurs se sont montrés moins amicaux. Un de ces «hackers» m'a, par exemple, contactée pour m'offrir généreusement toute sa collection du fanzine hacker *2600* afin de documenter ma recherche. J'étais ravie, et nous nous sommes donné rendez-vous dans un café de New York. Mais lorsqu'il a pris connaissance du sujet de mon livre, cet homme courtois, qui devait approcher la mi-quarantaine, a changé d'attitude. En maugréant «configurer Linux, ce n'est pas du hacking», il s'est levé et m'a plantée là. Cela dit, c'était presque agréable en comparaison du jour où un hacker m'a contacté en ligne pour me dire qu'il venait de voir ses collègues comploter contre moi sur IRC, avec dans l'idée de s'immiscer dans mon ordinateur afin de me montrer ce dont les vrais hackers sont capables. Oui, rien ne vaut une démonstration pratique pour soutenir un argument. Paniquée, j'ai verrouillé mes systèmes de sorte à me sentir en sécurité. J'imagine que le type qui m'avait prévenue a su refroidir les ardeurs des donneurs de leçon.

Évidemment, tous les hackers spécialisés en sécurité ne s'opposent pas farouchement à ce que leur titre s'applique aux développeurs de logiciels libres ou *open source*. Nombreux sont ceux qui utilisent et créent eux-

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

mêmes de tels programmes. L'un d'eux, David Mirza, établi à Montréal, a consacré de longues heures à m'expliquer les principes esthétiques et politiques complexes qui animent l'underground hacker. Cet ancien *black hat*, qui dirige aujourd'hui une firme de sécurité, est un défenseur infatigable de l'informatique à code source ouvert.

Mais il existe des différences, et elles sont de taille. Une bonne partie des hackers qui veillent à la sécurité informatique de l'État ou des grandes entreprises font face à des défis herculéens dans leur travail, qui consiste à sécuriser des applications, des systèmes d'exploitation, des serveurs et des réseaux. La tâche exige avant tout de comprendre l'état d'esprit de tout intrus potentiel – ce qui implique souvent de se livrer soi-même à des intrusions. C'est pourquoi les meilleurs hackers spécialisés en sécurité sont d'anciens *black hats* qui, à l'occasion, s'activent dans des zones grises sur le plan juridique. Ces hackers ont tendance à être un tantinet paranoïaques, ce qui n'est pas très étonnant: qui ne le serait pas, qui passerait son temps à peaufiner ses propres capacités d'intrusion, d'une part, et à chasser les fraudeurs de cartes bancaires, les associés du Russian Business Network, les auteurs de virus bulgares, les hackers au service de l'État chinois et les centaines d'autres vilains qui tentent sans relâche de s'insinuer dans des systèmes de grande valeur, d'autre part? En portant le fardeau de la paranoïa, les hackers chargés de la sécurité informatique permettent au reste de la population de dormir un peu mieux. (Mais il est préférable de ne dormir que d'un œil, car leurs conseils ne sont pas toujours suivis à la lettre.)

Quiconque a déjà fréquenté ces milieux sait que, pour ce qui est des technologies, les hackers de tout acabit sont d'incorrigibles snobs. Cette attitude n'alimente pas seulement l'antagonisme entre hackers spécialisés en sécurité et évangélistes du logiciel libre, et elle n'est d'ailleurs pas exclusive au monde des hackers. L'arrogance professionnelle est un trait répandu chez les gens de métier, qu'il s'agisse des médecins, des enseignants, des universitaires, des journalistes ou des ébénistes. La condescendance est un art qui pousse la personne qui en use à se surpasser. Toutefois (pour des raisons qui m'échappent encore), si on le compare à

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

celui d'autres spécialistes qu'on pourrait aussi qualifier de «hackers», l'élitisme des experts en sécurité informatique atteint des sommets inégalés. Ces hommes et ces femmes n'ont vraiment pas l'éloge facile.

Ce portrait sommaire du milieu de la sécurité informatique, auquel s'ajoute son mépris proverbial envers Anonymous, nous permet de mieux comprendre en quoi l'admiration que ses acteurs vouent à LulzSec est digne de mention. Et rien ne témoigne mieux de ce respect que la photo ci-dessous, prise en 2011 lors d'une fête d'Halloween[17].

Vêtus comme «le sir» de LulzSec, ces hackers de New York ne font pas que se taper un délire: ils affichent leur soutien aux hackers rebelles de la marge. Mais si tous les symboles de la mythologie de LulzSec sont là, un élément s'y ajoute – ou plutôt s'y retranche –, lequel ne saute pas aux yeux: l'absence de pantalons. De nombreux observateurs considèrent que LulzSec cherche à montrer, dans le plus pur style crasseux d'internet, que le roi est nu. Juchés au sommet d'une montagne isolée et balayée par les vents d'où personne ne les entend, les experts insistent depuis toujours sur l'impérieuse nécessité d'investir plus de ressources, d'énergie, de temps et de personnel

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

dans l'amélioration de la sécurité informatique. LulzSec semble enfin avoir trouvé le moyen de faire passer le message.

On peut se demander pourquoi la sécurité est à ce point déficiente dans un domaine à tel point immense et rentable. C'est que (les craintes à) ce sujet alimente(nt) un marché florissant[18]. L'industrie n'a de cesse de proposer des logiciels douteux (comme ces solutions clés en main impossibles à configurer en fonction des risques particuliers auxquels une organisation est exposée) ou des produits dont elle prétend qu'ils sont capables de remplacer toute une équipe de spécialistes, mais qui font souvent plus de tort que de bien. À cela s'ajoute le fait que, pour bon nombre d'entreprises, y compris parmi les plus prospères, la sécurité est loin d'être une priorité. «Un des défis pour les professionnels de la sécurité informatique consiste à amener les gens à la prendre au sérieux. Les cadres n'y voient qu'une dépense», explique un hacker spécialisé de New York. Le simple fait qu'en 2011, Sony, une société multinationale, ait pu être pillée sans vergogne en dit long sur la nature et l'ampleur du problème. Ce sont des cas comme celui-là qui rendent furieux les créateurs de systèmes sécurisés.

De mémoire récente, plus que tout individu, rapport ou autre groupe, LulzSec est parvenu à faire passer un message que bon nombre de professionnels de la sécurité informatique martelaient en vain depuis plus de vingt ans. La portée de ses actions rappelle les facéties de L0pht Heavy Industries, une association informelle de hackers qui, dans les années 1990, se rencontraient régulièrement. En 1998, lors d'une discussion de groupe, quelques-uns avaient introduit le terme *gray hat* pour décrire les hackers occupant (délibérément) une position ambiguë entre les *black hats* et les *white hats*, respectivement mal et bien intentionnés. Encore aujourd'hui, les *gray hats* n'hésitent pas à agir dans l'illégalité, mais ils le font généralement dans le seul but de détecter des vulnérabilités et de les faire connaître. L0pht a connu un tel succès qu'en mai 1998, la commission du Sénat des États-Unis sur la sécurité intérieure et les affaires gouvernementales, alors dirigée par le républicain Fred Thompson, a invité sept de ses membres à témoigner (ce qu'ils ont fait de façon un peu théâtrale). Avec son accent du

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Tennessee, le sénateur Thompson a présenté le «groupe de réflexion de hackers» en précisant que, «vu la nature délicate des activités de L0pht, ses membres interviendront sous leurs pseudonymes de hackers: Mudge, Weld Pond, Brian Oblivion, Kingpin, Space Rogue, Tan et Stefan von Neumann[19]». Des ricanements se sont fait entendre dans la salle, sans doute parce que ce recours à des pseudos était superflu: la chaîne C-SPAN enregistrait la séance et les hackers ne portaient pas de masque. Ces derniers ont abordé de nombreux sujets, mais ils ont été l'objet d'une attention particulière lorsqu'ils ont déclaré être en mesure de paralyser internet en une demi-heure. Il ne s'agissait pas d'une menace, mais plutôt d'un plaidoyer pour l'amélioration de la sécurité du réseau, horriblement déficiente en 1998.

Le témoignage de L0pht devant la commission était empreint de déférence; la plupart de ses membres portaient un complet, et le groupe a pris soin de fournir des explications à la portée du plus grand nombre. LulzSec, au contraire, ne sera jamais invité au Congrès – et n'était pas en mesure de paralyser internet –, mais, au fil de leur odyssée, ses membres réussiront à transmettre un message similaire. Ils réussiront à attirer l'attention sur l'état lamentable de la sécurité d'internet, non pas avec un témoignage soigneusement préparé, mais simplement au gré de leurs aventures en mer (lors desquelles ils auront mené au moins une dizaine d'opérations de hacking remarquées). Ils le feront au mépris de lois américaines comme la CFAA, conçues pour punir tout hacker pris sur le fait, quelles que soient ses motivations. Les opérations audacieuses de LulzSec contre de grandes entreprises et des agences de l'État, lesquelles deviendront légendaires, s'avéreront très efficaces (et sans doute nécessaires) pour réveiller les consciences.

De nombreux experts en sécurité informatique que j'ai interviewés considèrent que LulzSec a amené les cadres supérieurs à les écouter, du moins pendant une brève période (l'année 2013 est marquée par une série d'atteintes à la protection des données: Adobe, Target, Neiman Marcus, LivingSocial, le bureau du greffe de l'État de Washington, Evernote, Drupal.org, la Réserve fédérale des États-Unis, OKCupid, et ainsi de

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

suite[20]). En 2011, un billet de blog du journaliste et chercheur en sécurité Patrick Gray intitulé «Why We Secretly Love LulzSec» (Pourquoi nous aimons secrètement LulzSec), qui traduit très bien l'état d'esprit des experts du domaine, connut un vif succès chez ces derniers. Gray me parlera plus tard de la réception de son texte: «Il a créé un plus grand buzz que tout ce que j'avais écrit auparavant, y compris des articles pour *ZDNet*/*CNet*, *The Sydney Morning Herald*, *The Age* ou *Wired*. [...] Plusieurs de mes papiers avaient connu un succès planétaire, mais, pour celui-là, c'était tout autre chose.» Voici un extrait de l'article en question: «Ceci pourra surprendre les non-initiés, mais les experts en sécurité prennent secrètement plaisir à voir ces types péter les plombs. [...] Les grands médias s'amusent à critiquer Sony pour ses lacunes en matière de sécurité, mais, honnêtement, peut-on croire un instant que le réseau XBox Live ne pourrait subir le même sort? (Je sais que la fuite du PSN n'est pas attribuable à LulzSec, mais l'argument reste valable.) Existe-t-il une seule cible qui ne puisse être atteinte[21]?»

Même si les innombrables problèmes de sécurité qui affligent internet ne peuvent être réglés par magie, les experts sont tout de même enchantés de lire un texte dont l'auteur ose se saisir de cette «patate chaude».

La performance de LulzSec révèle aussi l'hypocrisie de nombreuses firmes, qui se livrent à d'étranges acrobaties pour rejeter la responsabilité du problème sur autrui. Un chercheur new-yorkais en sécurité informatique qui préfère conserver l'anonymat explique: «Il est intéressant de constater que ces entreprises se font hacker tous les jours, mais que les renseignements qui leur sont subtilisés ne sont pas semés à tout vent sur internet. Les gens qui mettent la main dessus sont généralement motivés par l'appât du gain. L'ironie de la chose, c'est que, si quelqu'un viole leur propriété intellectuelle en vue d'obtenir quelque avantage financier, elles restent les bras croisés. [...] Bref, LulzSec met les gens au pied du mur.»

Chris Wysopal, un membre fondateur de L0pht qui dirige aujourd'hui une firme de sécurité réputée, va dans le même sens:

> Les entreprises se préoccupent plus de leur image publique que de leur propriété intellectuelle. Les attaques contre Sony ont donné des sueurs

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> froides aux responsables de la sécurité des systèmes d'information et aux conseils d'administration des sociétés figurant au palmarès Fortune 100. Des clients sont venus nous voir en nous disant: «Je ne veux pas faire de moi un autre Sony.» Pour éviter de connaître un tel sort, ils ont passé au peigne fin des milliers de sites web et corrigé des centaines de vulnérabilités critiques. C'est ainsi que LulzSec a réussi à rendre internet plus résistant. À certains égards, on peut comparer son intervention à une vaccination, qui donne au système immunitaire un avant-goût d'un virus mortel et stimule les défenses de l'organisme.

Si LulzSec est populaire chez les experts en sécurité informatique, ce n'est pas seulement parce que le groupe a su mettre les cadres «au pied du mur». Son iconographie riche et à la portée de tous témoigne du plaisir de la subversion et de la magie du hacking, si souvent invisibles. On pourrait croire que le codage, le craquage, la sécurisation et les tests d'intrusion n'ont rien à voir avec l'art, la créativité et le plaisir, mais c'est là précisément ce que vivent ces technologues: de la béatitude (sans oublier cette forme de frustration atroce qui rend la joie deux fois plus intense lorsqu'elle est dépassée). Expliquer la nature d'une telle satisfaction aux non-initiés frise l'impossible, vu le caractère hautement ésotérique du savoir-faire en jeu. Jamais je n'ai vu représentation plus fidèle de l'esthétique, de l'ambiance et de la sensibilité propres au plaisir du hacking que dans les facéties de LulzSec. Et chaque élément de l'iconographie du groupe symbolise les dimensions sensuelle et idéologique de cet univers: le navire (la liberté des pirates au long cours), le gentleman au monocle et au costume trois-pièces (le hacker snob et prétentieux), le chat (s'il y a un lien avec internet, il doit y avoir des félins), la musique (il est toujours préférable de hacker sur de la musique que dans le silence), les manifestes (la liberté d'expression, bon sang!) et l'illégalité (parce que les règles, on n'en a rien à foutre). Plus que tout autre groupe, LulzSec incarne le plaisir du hacking et de la subversion. Le groupe incarne aussi le désir et le fantasme: ses membres accomplissent ouvertement ce que beaucoup de hackers *auraient eux-mêmes espéré* accomplir. Certains d'entre eux ont

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

sans doute goûté aux mêmes plaisirs illicites il y a belle lurette, quand les portes de l'informatique s'ouvraient à eux grâce à leurs explorations et à leurs bidouillages, mais cela ne se faisait généralement pas sous le regard d'un vaste public.

Cela dit, ce ne sont pas tous les hackers qui se pâment pour LulzSec. HTP, le groupe qui se plaisait à attaquer Anonymous, a étendu sa haine au rejeton du collectif. «HTP nous considérait comme une bande de crétins prêts à tout pour attirer l'attention», dira pwnsauce, un membre de LulzSec. L'opinion de ces rivaux reflète une philosophie bien enracinée dans l'underground hacker, laquelle amène certains hackers à traiter sans ménagement ceux de leurs pairs qui cherchent à attirer l'attention des grands médias (la quête d'attention relève de l'hérésie, et les manquements de LulzSec à cet égard démontrent le bien-fondé de cette sagesse populaire). Même si les membres de LulzSec accordent peu d'interviews, ils font tout pour attirer l'attention en vue de décrocher des articles importants. Ils iront même jusqu'à attaquer les médias eux-mêmes.

Les médias

Le collectif Anonymous n'a peut-être jamais (volontairement) eu de porte-parole, mais il dispose d'un canal IRC public, #reporter, où des dizaines de journalistes ont pu interviewer des participants. LulzSec est plus secret. Il n'a pas de canal public ouvert aux journalistes et ne donne pratiquement jamais d'interviews (sauf à Parmy Olson et, à l'occasion, à Steve Ragan). Aucune vedette n'est mise à l'avant-plan, outre le groupe en tant que tel. Néanmoins, à la fin juin 2011, LulzSec est en quelque sorte devenu un groupe de rock stars du hacking. Son incursion dans l'univers de la célébrité fait froncer les sourcils de certains Anons, mais, dans l'ensemble, la distance est assez grande entre LulzSec (qui a maintes fois confirmé son autonomie) et Anonymous, si bien que ce dernier peut profiter du spectacle sans avoir l'impression qu'on bouleverse ses habitudes et sa sensibilité éthique.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Contrairement à AnonOps, LulzSec n'épargne pas les médias. Sa grande opération de hacking contre la presse aura pour cible le réseau de télévision PBS, en représailles à la diffusion, dans le cadre de l'émission *Frontline*, d'un film sur WikiLeaks intitulé *WikiSecrets*. Ce documentaire a suscité la colère des membres de LulzSec, en particulier de Sabu, qui l'a détesté parce qu'on y élude les enjeux politiques pressants soulevés par la divulgation des câbles diplomatiques et qu'on y pose un regard sensationnaliste sur la psyché «obscure» de Chelsea Manning. LulzSec lance alors une campagne en deux volets: ses membres subtilisent les données personnelles d'employés de PBS et défacent le site web de la chaîne, où ils publient un faux article très réussi (voir l'encadré suivant).

Même si l'article devait être perçu comme faux, il marche alors comme canular. Sans doute parce que l'histoire qu'il raconte semblait plausible, Topiary, son auteur, l'a truffé d'indices révélant sa nature factice – à commencer par la source de l'information, un journal intime rédigé à la main, qui est pour le moins désuète. Le passage le plus incroyable est celui où il laisse entendre que les autorités respectent l'arrangement – non seulement parce que la vie privée est une denrée rare pour les célébrités, mais aussi parce qu'elle n'existe plus depuis un bout de temps. Les lecteurs qui se seraient laissé berner sont enfin ramenés à la réalité par un bout de phrase sans queue ni tête, «l'abattoir à yaks au puy vain» (une anagramme des noms des participants à l'opération, à savoir Topiary, Sabu, Kayla et Avunit), et une référence à la conjointe de l'auteur du journal intime, Penny (le prénom de nulle autre que la présidente de HBGary).

PBS NEWSHOUR

Topics | Video | Recent Programs | Teacher Resources

The Rundown — A BLOG OF NEWS AND INSIGHT

TUPAC -- May 29, 2011 at 11:30 PM EST

TUPAC TOUJOURS VIVANT, EN NOUVELLE-ZÉLANDE

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Le célèbre rappeur Tupac a été aperçu vivant dans une petite station balnéaire de Nouvelle-Zélande, rapportent des habitants de l'endroit. La petite ville, que nous ne nommerons pas pour des raisons de sécurité, hébergerait Tupac et Biggie Smalls (un autre rappeur) depuis plusieurs années. Un de ses résidents décédé récemment, David File, a laissé un journal intime contenant des preuves et des témoignages d'une visite de Tupac. À sa demande, celui-ci a été expédié à sa famille qui vit aux États-Unis.

«Ce que David nous a laissé nous a stupéfaits, a déclaré une de ses sœurs, Jasmine, 31 ans. Nous avons cru bon de diffuser l'information, car nous jugeons qu'elle mérite de ne pas rester confidentielle.»

Âgé de 28 ans, David a été tué lors d'une fusillade déclenchée par des membres locaux du crime organisé. Il a reçu plusieurs balles en rentrant du travail et a été retrouvé mort sur les lieux du crime. La police a trouvé son journal dans le tiroir de sa table de chevet.

«Naturellement, nous n'avons pas lu le journal de David, a déclaré un policier. Nous avons simplement pris note de sa demande de l'envoyer à une adresse située aux États-Unis, ce que nous avons fait, dans le respect de son souhait.»

Les autorités, qui ont bouclé la ville, refusent de se prononcer sur l'hypothèse selon laquelle Tupac ou Biggie auraient été emmenés dans une autre région ou un autre pays. Quant aux habitants du coin, ils se refusent à tout commentaire sur la durée du séjour des rappeurs. «Nous ne parlons pas de ça ici», s'est contenté d'affirmer l'un d'eux.

La famille de David File exige pour sa part qu'on fasse tout le nécessaire pour arrêter les responsables de la fusillade. «David était un garçon adorable et innocent, a déclaré sa mère. Depuis qu'il s'était établi en Nouvelle-Zélande, il n'avait jamais été aussi heureux.»

Son frère Jason a demandé qu'une partie du journal de David soit rendue publique afin qu'elle soit déchiffrée. «Vers la fin, a-t-il raconté, on tombe sur un passage, "l'abattoir à yaks au puy vain", que nous ne sommes pas encore parvenus à comprendre.»

La conjointe de David, Penny, n'a pas voulu faire de déclaration.

MAKE A COMMENT (0) | RETWEET FACEBOOK BUZZ SHARE

Bien que ce défaçage du site d'un média en dérange certains, la rapidité avec laquelle la nouvelle se répand sur Twitter témoigne, il faut le dire, d'une certaine admiration. On peut expliquer l'attrait d'une telle opération à l'aide de la définition anthropologique du vandalisme que propose Michael Taussig dans son remarquable essai sur le sujet,

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Defacement: «Le vandalisme est aux objets ce que les blagues sont à la langue: il fait ressortir leur magie intrinsèque, d'autant plus si l'objet en question est devenu banal[22].» Avec une forte dose d'humour, LulzSec a mis à nu le thème de la célébrité en vandalisant un objet médiatique, l'article journalistique.

Tous les grands médias occidentaux publient quelque chose sur l'article bidon, mais la plupart d'entre eux effleurent à peine la subtilisation des données, douteuse sur le plan éthique, et la motivation politique des hackers, même si LulzSec a publié une déclaration précisant explicitement ses intentions. Voilà qui démontre une fois de plus (et non sans ironie) la propension des médias à dramatiser les enjeux –, une propension elle-même affichée par les créateurs du documentaire sur WikiLeaks qui a poussé les hackers à lancer l'opération.

«Nous explorons l'avenir»

On pourrait penser que la plupart des grandes entreprises voient LulzSec (et, par extension, Anonymous) d'un mauvais œil. La réalité est un peu plus nuancée. À partir de l'automne 2011 (avec un point culminant en 2012), diverses personnes et organisations appartenant aux plus hautes sphères des milieux d'affaires se sont mises à me contacter. Ainsi, j'ai parlé avec un associé-fondateur d'une société de capital-risque basée à New York, au directeur européen de la sécurité de Vodafone et au premier vice-président de TTI/Vanguard («un forum sans équivalent, destiné aux cadres supérieurs, qui associe la planification stratégique en matière de technologie à la réussite en affaires»). J'ai aussi prononcé deux conférences (dont une vidéoconférence) pour un groupe de l'université de New York consacrées aux risques et à la sécurité, auxquelles ont assisté des chefs de la sécurité et d'autres cadres de grandes entreprises. Enfin, j'ai participé à un événement organisé par World 50, une association regroupant les cadres supérieurs de sociétés figurant pour la plupart au palmarès Fortune 500.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

La liste serait incomplète sans une mention de ma participation à l'édition 2012 des conférences TEDGlobal, à Édimbourg, en Écosse. Bien que les conférences TED soient suivies par des millions de personnes grâce à leur diffusion en ligne, elles sont essentiellement fréquentées par de riches membres de l'élite, si l'on fait exception de certains orateurs, dont moi-même, et de participants triés sur le volet qui reçoivent une aide financière de l'organisation. L'inscription, pour laquelle on doit bien sûr avoir été sélectionné (après en avoir fait la demande), coûte quelque 6 000 dollars, un privilège qui n'inclut pas les frais de déplacement et d'hébergement, mais permet de prendre part à des soirées chic où abondent nourriture et boisson, à des concerts et à des conférences sophistiquées, et de discuter avec des célébrités (ou, à tout le moins, avec leurs assistants). À la suite de mon exposé, l'assistant personnel de Will Smith est venu me faire la conversation. Il a tenté de me convaincre que son patron, qu'une rumeur associe à la Scientologie, est en fait un fan inconditionnel d'Anonymous. S'agissait-il d'une manœuvre destinée à protéger Smith contre une éventuelle attaque du collectif, laquelle pourrait nuire à sa carrière, ou d'une rencontre véritablement fortuite?

Mais une autre rencontre a été bien plus mémorable encore. Alors que je profitais d'une pause pour déguster un des succulents petits fours, un cadre «Fortune 500» m'a pris par le bras (un peu trop fermement à mon goût) et, projetant manifestement son anxiété sur moi, m'a chuchoté assez fort à l'oreille: «Je vous trouve *teeeeeellement* courageuse d'étudier Anonymous!» La veille, j'avais rendu visite à un Anon d'Édimbourg et à sa compagne. Après m'avoir fait visiter leur jardin, où se trouvait une ruche, ils m'avaient convié à leur table pour déguster un faisan accompagné d'une purée de patate douce, puis nous avions regardé ensemble le documentaire *We Are Legion: The Story of the Hacktivists.* Mon hôtesse avait été étonnée d'apprendre qu'Anonymous avait une teneur politique, elle qui croyait que son homme ne s'affairait à son ordinateur que pour prendre part à des activités puériles. J'avais passé un moment si agréable en compagnie de ce «redoutable» Anon qu'il m'était difficile d'accepter les éloges de bravoure

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

dont me couvrait ce capitaine d'industrie. *Il est vrai que j'aurais pu me faire piquer par une abeille*, me suis-je dit.

À certains égards, ces hommes et ces femmes présents à la conférence m'ont semblé des gens ordinaires. Ils se plaignaient de leurs enfants gâtés, du coût exorbitant des études supérieures et (pour certains d'entre eux, du moins – un immigrant canadien, si je me souviens bien) de l'absence d'un système de soins de santé universel aux États-Unis. Certains se sont même adonnés à ce bon vieux passe-temps prisé par tous les milieux de travail: la médisance sur son supérieur immédiat. Il va sans dire que, là où je me trouvais, ce dernier était généralement PDG d'une grande boîte. Mais qu'on ne s'y méprenne pas: pendant l'événement de World 50 au Contemporary Jewish Museum de San Francisco, j'ai surpris deux serveurs dans la vingtaine murmurer, sans se soucier de mon oreille indiscrète: «C'est un autre monde, ici.» Prenons l'exemple des porte-noms distribués pour l'événement. Ceux-ci n'avaient rien de ces petits cartons glissés dans un support en plastique retenu par quelque cordon orné de logos. On aurait plutôt dit qu'ils venaient tout droit de chez Restoration Hardware (une chaîne américaine de magasins de meubles haut de gamme). Pourvus d'un fermoir métallique aimanté, ils auraient pu à la rigueur servir de *shuriken* à un ninja. Le mien, hélas, ne m'aura servi qu'à décliner mon identité. Après qu'on nous eut remis nos porte-noms et servi un déjeuner de thon poêlé accompagné d'autres mets fins, on nous a emmenés à l'étage dans la vaste salle privée, baignée de soleil et pourvue de fauteuils moelleux, où allaient avoir lieu les conférences, dont les thèmes allaient des cours en ligne ouverts à tous à Anonymous (la mienne, bien sûr). L'auditoire était constitué de dirigeants d'AstraZeneca, de Cargill, de Hewlett-Packard, de Hilton Worldwide, de Huwaei Technologies, de Hyatt Hotels, de Juniper Networks, de Monsanto, de Rio Tinto, de Coca-Cola et de Tiffany & Co. Même si un repas venait tout juste de nous être servi, la salle regorgeait de mets divers, dont de superbes verres pleins de M&M et une dizaine de boissons différentes. Aussitôt les exposés terminés, tout le monde a été convié à un restaurant avec vue sur le Bay Bridge pour un dîner précédé d'une causerie intime avec Steve Martin.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Lors de ma conférence, sans surprise, il m'a semblé que les cadres, et en particulier ceux des plus grandes sociétés, ne souhaitaient rien davantage que de voir quelqu'un lever sa baguette magique pour faire disparaître Anonymous et LulzSec. Ceux des entreprises de nouvelles technologies m'ont semblé plus curieux, à tout le moins conscients de la participation d'Anonymous à divers mouvements politiques. Ils ont même fait montre d'un certain intérêt pour le rôle du collectif dans le Printemps arabe. Les cadres des secteurs de la finance et de l'énergie, eux, se sont montrés assez froids, tandis que ceux des autres secteurs affichaient un curieux mélange de dégoût et de crainte. La directrice des communications d'une compagnie aérienne *low cost* a souhaité, à la blague, se faire hacker par Anonymous: la publicité gratuite qui en résulterait serait fabuleuse!

Le plus inattendu fut lorsqu'on m'interrogea sur l'apport que pourrait offrir Anonymous au monde de la grande entreprise. Un représentant de TTI/Vanguard m'a approchée pour m'inviter à donner une conférence à ce sujet à ses clients, dont faisaient partie Royal Dutch Shell, Northrop Grumman, Toyota, FedEx et Expedia. Cela m'a permis d'apprendre que la mission première de TTI/Vanguard consistait à «explorer l'avenir». L'organisation affirmait «pousser plus loin la réflexion sur les possibilités recelées par les technologies. Nous explorons l'avenir. Nous nous intéressons aux sources inattendues de changement, dont nous évaluons le potentiel transformateur. Nos séances dynamiques et très interactives stimulent le débat et favorisent l'émergence d'idées novatrices»[23].

On parle ici d'une culture qui adopte des stratégies «perturbatrices» au service de l'économie de l'attention, du gain en capital. Anonymous et LulzSec, eux, pratiquent la perturbation de façon classique, sans réserve. Il leur arrive même de foutre le bordel. Ils démontrent également l'importance de l'art, de l'expressivité, de l'autonomie et de la création par le travail non aliéné. La plupart des sociétés multinationales sont allergiques à ces idéaux; il leur est impossible de les mettre en œuvre, du moins pas de façon épanouissante et honnête.

C'est en lisant l'énoncé de mission de TTI/Vanguard que j'ai eu mon premier contact avec la notion d'«exploration de l'avenir»; par la suite, le

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

terme s'est mis à surgir de partout. Sa mention la plus étonnante est survenue pendant un appel téléphonique de Chris Anderson, l'administrateur de TED, quelque temps avant la conférence d'Édimbourg. Il m'a demandé si, dans mon exposé, je pouvais inclure des perspectives pratiques pour les gestionnaires d'entreprises. Bien que sa requête fût subtile, il souhaitait manifestement que je relaie des connaissances (hyperinspirantes, étonnantes, perturbatrices), acquises dans les tranchées d'Anonymous, capables d'ébranler les croyances populaires et de stimuler la réflexion entrepreneuriale. Jusque-là, j'avais surtout travaillé avec l'autre administrateur de l'organisation, Bruno Giussani. TED vérifie tout jusqu'au moindre mot (par exemple, Bruno Giussani m'avait demandé d'éviter le terme *homeland* [patrie] parce qu'il le jugeait trop connoté politiquement). Pour le reste, Giussani m'avait laissé carte blanche et y était allé de suggestions que j'étais libre de retenir ou de rejeter. J'ai donc été franchement surprise par la requête d'Anderson. De toute évidence, adopter la langue de bois des milieux d'affaires en présentant Anonymous comme un phénomène épatant, en utilisant des formules creuses, mais bien tournées, et en annonçant l'avènement d'un nouveau paradigme, le tout dans un jargon techno nébuleux et avec une exaltation électrique, était la recette parfaite pour donner à ces robots gestionnaires l'impression de prendre part au *brainstorming* du siècle. J'aurais ensuite pu gagner beaucoup d'argent en récitant mon boniment jusqu'à l'émergence d'un autre «nouveau paradigme».

Ces échanges m'ont permis de porter un regard neuf sur la question contemporaine de la récupération. Les intellectuels qui écrivent sur le sujet l'abordent souvent à partir de la publicité, du divertissement et de la consommation – l'exemple classique étant cette étude pionnière de Dick Hebdige sur la marchandisation de la culture punk[24]. La force critique de la contre-culture, dont le punk est emblématique, a été totalement dévitalisée par son passage dans l'appareil publicitaire et son formatage par Hollywood et l'industrie de la mode. Ce que j'ai toujours trouvé intéressant à propos d'Anonymous, c'est à quel point le collectif a pu résister, du moins jusqu'à tout récemment[25], à ces forces. La raison principale en est que la

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

plupart des grandes entreprises hésitent à marchandiser le collectif parce qu'elles savent quelles conséquences immédiates elles pourraient en subir. En fait, le cas d'Anonymous est particulier en ce qu'il illustre le plus souvent un processus de récupération inverse: s'il est vrai que Time Warner gagne de l'argent chaque fois qu'une personne achète un masque de Guy Fawkes (le conglomérat détient les droits du film *V pour Vendetta*), Anonymous s'est néanmoins approprié un symbole popularisé par Hollywood et l'a rendu révolutionnaire. Il s'agit là d'un exemple éloquent de contre-marchandisation, un phénomène rare.

Mais s'il y a une leçon à tirer des méthodes des dirigeants de grandes sociétés, c'est celle-ci: même s'ils ne sont pas à la veille de s'approprier l'imagerie d'Anonymous pour une campagne de pub, cela ne signifie pas qu'ils ne peuvent pas trouver une façon de s'approprier un *aspect* d'Anonymous. Quiconque tombe sur une idée non encore capitalisée, exploitable, porteuse d'avenir, novatrice et dérangeante, qui puisse faire son chemin dans la salle d'un conseil d'administration, tentera de la mettre en valeur. Une telle manœuvre, qui se distingue des formes habituelles de récupération – dans la mesure où le transfert de connaissances n'altère pas (nécessairement) le phénomène observé –, devrait tout de même être étudiée d'un peu plus près. Il existe une industrie florissante et omniprésente (groupes de réflexion, organisations et spécialistes de la motivation souvent venus du monde universitaire, en particulier ces experts qui aiment à gonfler les promesses de la technologie), dont la mission consiste à se saisir d'idées émanant de tous les milieux et de tous les coins du monde (des gangs de rue au Printemps arabe) en vue de les convertir en opportunités. Son objectif consiste à aider les dirigeants des grandes sociétés à se tenir au courant des enjeux mondiaux, à être fiers de ce qu'ils font, à renforcer leur machine culturelle et à tirer de juteux profits d'une culture dans laquelle ils n'ont pas besoin d'investir. Dans certains cas, j'ai l'impression que les cadres qui s'intéressent à un phénomène comme le logiciel libre acquièrent non seulement des idées payantes pour leur entreprise, mais aussi le pouvoir de façonner l'opinion du public sur le sujet. On ne sait pas grand-chose sur la portée de ces réseaux et les effets

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

potentiels de l'«exploration de l'avenir». Le sujet mériterait sans aucun doute d'être mieux compris. On devrait peut-être «explorer l'avenir» de l'exploration de l'avenir.

«Je vous le dis, il faut avoir encore du chaos en soi pour enfanter une étoile dansante[26].»

LulzSec n'a pas seulement suscité l'engouement des hackers. Le groupe a aussi acquis une grande popularité auprès des geeks d'internet, des militants et des universitaires, de même que chez bon nombre d'observateurs lambda. Un philosophe allemand du XIX^e^ siècle peut nous aider à comprendre pourquoi: Friedrich Nietzsche remet en question la vérité et la morale, élève le plaisir au-dessus de la raison, embrasse la ruse et l'hyperbole. Ne peut-on pas y voir (sans trop se prendre au sérieux) le fondement intellectuel de l'œuvre accomplie par LulzSec et Anonymous cent-cinquante ans plus tard? (Je crois d'ailleurs que, si Nietzsche avait été téléporté dans le futur et s'était mis au hacking, il se serait joint à LulzSec.)

Nietzsche avait tellement à cœur le projet critique des Lumières qu'il a fini par en devenir un des critiques les plus acharnés, contribuant ainsi à l'avènement d'une philosophie radicale qui prendrait son essor au XX^e^ siècle chez tout un cortège de penseurs, dont les plus célèbres sont Gilles Deleuze, Félix Guattari et Michel Foucault. On pourrait presque qualifier Nietzsche de *trickster* des Lumières. Sa critique prend pour objet la raison, le progrès, Dieu, la science et la façon dont les idées ou les systèmes fondés sur des absolus (peu importe qu'ils proclament la vérité de la science ou celle de Dieu) deviennent, une fois adoptés par le plus grand nombre, plus résistants à la critique et plus aptes à retenir les hommes sous leur emprise. Pour Nietzsche, rien ne doit être tenu pour acquis ou déterminé à priori: ni le bien ni le mal, ni le vrai ni le faux. Selon lui, tout élément de savoir conçu, créé ou découvert en observant le monde est provisoire, enraciné dans le jugement et, tout intemporel ou naturel puisse-t-il sembler, compréhensible uniquement à un moment déterminé de l'histoire.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Les raisons pour lesquelles Nietzche a pris d'assaut le bastion idéologique de la vérité, de la raison et de la morale sont complexes. Pour les besoins de cet exposé, contentons-nous de dire qu'il souhaitait révéler à quel point la chape de la vérité exerce un monopole. Qui dit vrai dit juste, mieux et bien. Tout ce qui est déclaré vrai se trouve ainsi à dévaloriser les autres domaines de la création et de l'expérience, dont l'art et le mythe, situés à l'extérieur de l'orbite de la «vérité» et donc classés dans la catégorie de la «fausseté». Cette antinomie fait de l'art un citoyen de seconde zone dans le monde des idées, où l'imaginaire et le mythe, eux, ont à peine droit de cité.

Nietzsche était à l'écoute de la vitalité des sens, du mythe et de l'art. Il considérait la musique, la poésie et même le rire sardonique du *trickster* Dionysos, qu'il défendait, comme les vecteurs d'une esthétique du plaisir[27]. Certaines quêtes permettent à l'être humain de surmonter ses limites et le caractère tragique de sa condition: «Ce n'est pas la colère, c'est le rire qui tue. Allons, sus à l'esprit de Pesanteur[28]!»

Plus que tout autre mouvement politique contemporain, Anonymous et surtout son rejeton LulzSec incarnent de façon frappante certains de ces thèmes nietzschéens. Nietzsche soutenait que rien n'est sacré et prônait une vie fondée sur l'enchantement; c'est là ce que LulzSec et Anonymous vivent pleinement. Subversifs, ils osent contrevenir à la loi, aux conventions sociales et aux bonnes mœurs en pratiquant l'art de la transgression. Ils rappellent à leurs concitoyens que, pour faire de la vie un art et rendre l'art vivant, on doit parfois enfreindre les règles.

Et contrevenir aux règles n'a rien d'une tâche facile. À l'époque où je donnais un cours sur la communication et la culture, je demandais à mes étudiants d'enfreindre une règle en public, puis de relater leur expérience au groupe. Sauf pour une poignée d'excentriques plutôt à l'aise avec une telle consigne (comme cette étudiante racontant que sa mère l'avait promenée en laisse dans les rues de New York sous le regard indifférent des passants), l'exercice s'est révélé extraordinairement difficile, pour ne pas dire douloureux. En fait, un bon quart de mes élèves se sont exécutés d'une façon qu'on pourrait difficilement qualifier d'«audacieuse» – en demandant

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

à quelqu'un si il ou elle pouvait s'asseoir à la même table de café, par exemple.

La pression sociale est très forte pour céder aux conventions et accepter les idées reçues, souvent pour de bonnes raisons. Une bonne partie de l'œuvre de Nietzsche dénonce cette tendance et constitue une mise en garde contre ses effets pernicieux; c'est aussi ce que font, d'une époque à l'autre et sous diverses formes, les mythes du *trickster*. Un des plus célèbres personnages du philosophe et poète, Zarathoustra, est d'ailleurs un genre de *trickster*. Vivant en ermite dans les montagnes depuis dix ans, il a réalisé qu'on peut surmonter les conventions sociales pour leur substituer des désirs et des idées qu'on définit par soi-même. Il descend de son refuge pour partager cette intuition avec ses pairs, vantant les mérites de ce qu'il qualifie de «victoire sur soi[29]». Anonymous et LulzSec sont en quelque sorte les héritiers de Zarathoustra. LulzSec est allé un peu plus loin en enfreignant les règles instituées au sein même d'Anonymous, et est ainsi devenu une menace pour cet ordre émergent.

Il est rare à notre époque qu'advienne quelque chose qui puisse être rapproché du mythe du *trickster*, d'autant plus avec un tel panache et une telle visibilité. Par leur sacrifice (et par le sacrifice d'autrui), ces hackers viennent rappeler la nécessité, le plaisir et les dangers de la subversion.

L'émerveillement ressenti par tant de gens à l'égard d'Anonymous et de LulzSec peut être éclairé par les propos de Walter Benjamin sur «la figure du "grand" criminel [qui], même si ses fins étaient repoussantes, a provoqué l'admiration secrète du peuple[30]». Cette admiration naît du fait que la criminalité révèle les limites du monopole de l'État sur la violence et de la force de la loi. LulzSec et Anonymous débordent cependant du cadre de la criminalité, et ce, même s'ils ne sont pas parvenus à quitter entièrement son orbite. Contrairement aux groupes criminels, le collectif et son rejeton n'agissent pas par appât du gain, et, chez Anonymous, une forte pression collective étouffe l'égoïsme, la quête de célébrité et la soif de reconnaissance. Anonymous a donné forme à la leçon nietzschéenne incarnée par Zarathoustra: traduire en actes le désir secret de se débarrasser (ne serait-ce que momentanément) des chaînes de la normativité et

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

d’atteindre à la grandeur – en mettant la volonté de puissance au service de finalités collectives et altruistes au lieu d’aspirations intéressées et individualistes. Pour paraphraser Nietzsche, le chaos artistique d’Anonymous et de LulzSec a mis au monde une étoile dansante.

Si vous trouvez que mon regard sur LulzSec et cette période de l’histoire d’Anonymous est empreint de romantisme, vous avez sans doute raison. Toutefois, la suite des événements montrera qu’il s’agissait là d’une lune de miel de courte durée. Nous pouvons maintenant aborder la mort de LulzSec et l’essor d’AntiSec. Nous verrons comment ce mythe stupéfiant va mal tourner lorsqu’Anonymous vivra une éclipse partielle, attribuable à une forme de culte de la personnalité.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Chapitre 9

AntiSec

PAR UNE JOURNÉE DE FÉVRIER 2011, un hacker de Chicago âgé de 26 ans s'est connecté au serveur Internet Relay Chat (IRC) AnonOps. «Enfin une discussion constructive!» se dit-il sans doute: Anonymous était alors en pleine campagne contre les célèbres frères Koch, importants donateurs du gouverneur républicain du Wisconsin, Scott Walker. En cet hiver glacial, des militants de tout le Wisconsin avaient convergé depuis les fermes et les usines vers le capitole de l'État pour protester contre un projet de loi du gouverneur qui priverait les fonctionnaires de leur droit à la négociation collective. Le jeune hacker observait ainsi Anonymous mener une attaque par saturation contre Americans for Prosperity (Américains pour la prospérité), un groupe de défense du libre marché, financé par les frères milliardaires.

À Chicago aussi, il faisait froid. Tourbillonnant aux coins des rues, s'engouffrant dans les corridors créés par les immeubles, le vent de l'hiver s'était emparé de la ville. Notre hacker, Jeremy Hammond, était connecté depuis vingt minutes à peine quand il perdit sa connexion internet. Il soupira, déplia nonchalamment son grand corps et traîna les pieds jusque dehors. Debout derrière la maison, les doigts engourdis par le froid, il tenta désespérément d'ajuster l'antenne wi-fi à laquelle était branché son ordinateur portable. Ce dernier était muni du logiciel Aircrack-ng, qui était en train de faire son possible pour craquer le réseau sans fil du voisin. Hammond ne bougeait pas. Il savait que le moindre mouvement pouvait

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

altérer le signal. L'horloge indiquait trois heures du matin, et il gelait ferme. Rentrer n'aurait rien changé rien, car la maison n'était plus chauffée depuis des mois. Une fois la connexion internet rétablie, le jeune homme retourna sur IRC, où il passa les heures suivantes, à la lueur bleutée de son portable.

Hammond lisait tout ce qu'il trouvait sur les activités militantes d'Anonymous, et quelque chose le tarabustait. Il s'identifiait au collectif, dont il aurait bien voulu faire partie. Cet activiste passionné était sans conteste un des «hacktivistes» américains les plus actifs, inébranlables et déterminés. À 20 ans, il avait intégré l'action directe à sa vie, puis il s'était fait arrêter à huit reprises lors de manifestations. Lors de la convention républicaine de 2004 à New York, il avait été interpellé pendant une action de protestation consistant à faire du bruit avec des tambours; il avait été aussi arrêté l'année suivante alors qu'il manifestait contre un groupe néonazi à Toledo, en Ohio, parce qu'il avait contrevenu à une ordonnance lui interdisant de prendre part à des manifestations. Plus récemment, en 2010, après qu'il eut brûlé un drapeau olympique pour dénoncer la candidature de Chicago aux Jeux de 2016, on l'avait condamné à dix-huit mois de probation et à cent-trente heures de travaux d'intérêt collectif. Hammond se dit fièrement anarcho-communiste, car il croit passionnément aux «collectifs sans chef, fondés sur la libre association, le consensus, l'entraide, l'autosuffisance et l'harmonie avec l'environnement[1]».

La neige avait depuis longtemps disparu quand, à l'été 2011, Hammond s'en est pris activement à des serveurs et à des sites web pour des raisons politiques. Ces gestes lui seraient fatidiques: un peu moins d'un an plus tard, il serait arrêté, puis condamné à dix ans de prison. Après son arrestation, nous avons communiqué par de bonnes vieilles lettres envoyées dans des enveloppes timbrées (Hammond collait ses timbres à l'envers). Et en septembre 2013, lors de notre première et unique rencontre face à face au centre correctionnel métropolitain de New York, où il était incarcéré, il m'a parlé de sa vie militante et de son engagement au sein d'Anonymous.

À mon arrivée sur les lieux, j'ai constaté que le jeune homme, vêtu d'une combinaison trop grande en toile marron, n'avait plus l'allure dégingandée du programmeur qu'il était. Il a appuyé ses robustes avant-bras

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

(signe le plus visible des 25 kilos de muscle qu'il avait acquis en prison) sur la table de la salle nue destinée aux entretiens avec les détenus. En guise de trame sonore, on pouvait profiter du bourdonnement des néons, dont l'éclat se réfléchissait sur le mur de parpaings. En plus d'avoir veillé à ce que la pièce soit dépourvue de toute qualité esthétique, les autorités carcérales avaient trouvé le moyen d'y faire régner un froid mordant.

C'est dans cette ambiance on ne peut plus agréable que Hammond m'a appris un tas de choses sur son passé. Au fil de notre discussion, je constaterai peu à peu qu'il avait développé ses compétences techniques à des fins expressément politiques.

*
* *

Élevé par son père avec son frère jumeau dans la proche banlieue de Chicago, Hammond était à peine sorti du berceau lorsqu'il est tombé dans les jeux vidéo. À 10 ans, il se mettait à programmer ses propres jeux, en QBasic, sur un ordinateur portable 10 mégahertz sous MS-DOS 6 et Windows 3.1. Peu de temps après, il faisait son entrée en ligne, où il a mis sur pied un canal IRC consacré au développement de jeux. C'est à cette époque qu'il a découvert les genres littéraires prisés des hackers, dont les *textfiles* (fichiers texte, aussi connus sous le nom de *philes**) et les fanzines. Le plus souvent, les *philes*, «qui servent à l'enseignement des techniques et de la philosophie de l'underground [hacker]» sont «des sources convoitées de savoirs interdits», observe Bruce Sterling[2].

La plupart de ces fichiers ne manquent pas d'audace et ont une connotation anti-autoritaire, comme en font foi leurs titres:

- Hacking Bank America BANKAMER.ZIP
- Hacking Chilton CHHACK.ZIP
- Recueil pour Hackers DIGEST.ZIP
- Guide Phortune 500 à Unix P500UNIX.ZIP
- Hacking Radio RADHACK.DOC

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

- Livre anarchiste ANARCHST.ZIP
- Formule Barbituriques BARBITURA.ZIP
- Terrorisme électronique ELECTERR.ZIP
- Verrous porte-documents MRSHIN.ZIP
- Autres tours à jouer aux crétins! PRANK.ZIP[3]

Hammond a dévoré ces documents en présumant (de façon erronée) que la plupart des autres hackers partageaient sa vision politique. Mais lorsqu'il est entré à l'école secondaire et qu'il a commencé à assister aux réunions du fanzine *2600*, il a été ramené à la réalité, et plutôt brutalement. Les autres participants, se souvenait-il, étaient de «super *white hats*» dont la conscience politique était à des lieues de sa sensibilité anticapitaliste naissante. Néanmoins, parce qu'il se considérait lui-même comme un hacker, il aimait à participer à ces rencontres. Il était conscient d'avoir quelque chose à apprendre au contact de ces gens.

Sa conscience politique a monté d'un cran quelques années plus tard, «lorsque Bush a volé l'élection, que le 11-Septembre a eu lieu et que le Patriot Act a été adopté». À l'âge de 20 ans, il a cofondé un site web de gauche, HackThisSite.org (hackez ce site), accompagné d'un fanzine intitulé *Hack This Zine* (hackez ce fanzine). Ces intitulés faisaient écho à *Steal This Book* (volez ce livre), le manuel-manifeste de la contre-culture des années 1960 écrit par Abbie Hoffman. (Notons que les membres du Youth International Party, les Yippies, sont à l'origine du premier fanzine de hackers et de *phreakers*, le *Youth International Party Line*, qui prônait le hacking d'AT&T, surnommé «Ma Bell», en tant que geste révolutionnaire. La publication qui y succéderait, *Technical Assistance Program* [*TAP*, programme de soutien technique] serait débarrassée de cette rhétorique ouvertement gauchiste.) HackThisSite.org traitait certes de sécurité informatique, mais aussi des tendances et des actualités politiques de gauche de diverses régions du monde. Il y était entre autres question du mouvement contre la guerre d'Afghanistan et de la menace potentielle pour la démocratie que représentaient les machines à voter numériques.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Même si Hammond faisait figure d'exception dans le milieu des hackers américains, le monde comptait assez de ses semblables pour que se constitue une petite – mais fougueuse – clique de guerriers technogauchistes. Son fanzine a contribué à la formation de toute une flopée de hackers de gauche. D'ailleurs, un des membres les plus politisés de LulzSec, Donncha O'Cearbhaill, était un lecteur de *Hack This Zine* avant de faire la rencontre de Hammond en ligne. Et quand ce dernier n'était pas en train d'écrire pour le fanzine, il mettait ses compétences techniques au service de ses objectifs politiques.

Au cours d'une de ses premières opérations de hacking, avant qu'il ne devienne membre d'Anonymous (en fait, avant même que le collectif n'associe son nom à des causes militantes), Hammond avait défacé un site web en y publiant un portrait de Guy Fawkes. Lorsqu'il m'a raconté cette opération, soulignant son amour pour le film *V pour Vendetta*, ses yeux bleus se sont mis à pétiller, et son visage pâle, à s'animer. La salle austère a soudain semblé baigner dans une atmosphère feutrée; je l'ai donc pressé de me donner plus de détails. Les voici.

L'histoire commence en mars 2006, un an à peine après que Hammond se fut lancé dans le hacking politique. Le jeune homme vient de s'associer à BrigadaElektronica, un collectif informel et anonyme de hackers de gauche. Ces derniers lancent alors une opération de hacking contre des sites web de l'État philippin, soit ceux de la police nationale, du palais de Malacañan (résidence officielle du président), du bureau du président et du collège de la Défense nationale, en solidarité avec les «11 de Sagada», un groupe de militants, dont des membres de De la bouffe, pas des bombes, accusés de terrorisme et détenus dans la province philippine de Luzon[4]. (De la bouffe, pas des bombes est un regroupement de collectifs de gauche qui servent des repas véganes et végétariens aux affamés.)

Hammond n'est pas le seul anarchiste en herbe à aimer la superproduction hollywoodienne *V pour Vendetta*, sortie le même mois que la campagne de soutien aux «11 de Sagada». L'antihéros du film porte un masque de Guy Fawkes. Ce dernier s'est d'abord fait connaître en Grande-Bretagne au XVII^{e} siècle lors de la conspiration des Poudres dont il

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

deviendrait en quelque sorte la figure emblématique. Sa vaine tentative de régicide est depuis lors commémorée lors d'une fête, la Nuit de Guy Fawkes, où l'on célèbre la continuité de la monarchie en allumant des feux de joie un peu partout au Royaume-Uni. L'auteur britannique Alan Moore a adopté ce personnage devenu légendaire pour en faire le protagoniste d'une bande dessinée dystopique, laquelle a été adaptée par Hollywood. C'est ainsi que le visage de Fawkes a fini par symboliser le terroriste-devenu-icône-de-la-résistance. Si tous les symboles font l'objet d'une diversité d'interprétations, certains sont plus malléables que d'autres: alors que le symbole de la paix ne peut représenter que cette position, le faciès souriant et silencieux du masque a acquis au fil des ans une multitude de significations avant de devenir le visage de la dissidence populaire.

En 2006, peu de temps après ses premières incursions dans le monde du hacking politique, Hammond est arrêté, puis écroué dans une prison fédérale jusqu'en 2008. Il a infiltré le système informatique de Protest Warrior, une organisation de droite dont la devise est *Fighting the Left, Doing it Right* (combattre la gauche, comme il se doit), et y a subtilisé des données de cartes de crédit. Parce qu'il ne s'en est pas servi, il est seulement mis en accusation pour l'intrusion, ce qui lui permet d'échapper à une peine plus lourde et à une amende comparable à celles qu'on inflige souvent aux fraudeurs. (À l'issue du procès, la poursuite, qui réclamait une peine de cinq ans de prison et une amende de 2,5 millions de dollars, fait ce commentaire: «Alors que Hammond tentait de faire de ce procès une affaire politique, nous souhaitions que celui-ci porte sur ce qui s'est réellement produit, à savoir un vol de numéros de cartes de crédit[5].») Condamné à vingt-quatre mois de prison et à 5 358 dollars d'amende, il est incarcéré dans un établissement à sécurité moyenne, où il passera dix-huit mois.

Lors de notre rencontre, Hammond me fera une confession étonnante. En 2008, alors qu'Anonymous adopte le masque de Guy Fawkes qu'il aime tant, le collectif ne l'inspire guère. À ses yeux, les Anons ne sont que de vulgaires *skiddies*, et la culture du «tout est permis» qui anime les trolls déviants (à qui il arrive de sombrer dans le racisme) est «aliénante». Mais il ne s'agit là que d'irritants mineurs en comparaison de son rejet plus global

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

du «hacktivisme». Après s'y être adonné pendant quelques années au prix de deux ans de prison, il se demande si, «en tant qu'écologiste [...], je n'ai pas alimenté la bête industrielle en privilégiant la technologie». Pour un temps, il répond par l'affirmative et se tient à l'écart.

Toutefois, l'émergence de WikiLeaks et, en particulier, la divulgation de documents par Manning lui font prendre conscience du potentiel de la technologie pour «lever le voile sur la criminalité». Au moment de sa condamnation pour avoir participé à une opération d'Anonymous, Hammond lui rendra hommage: «Elle a pris des risques énormes sur le plan personnel en divulguant ces renseignements; convaincue que le public a le droit de savoir, elle espérait que ses révélations aideraient à mettre un terme à ces pratiques abusives. Il est désespérant de voir avec quelle cruauté elle a été traitée en prison militaire.»

Hammond commence à voir Anonymous d'un bon œil début 2011. C'est au cours de l'opération Wisconsin qu'il se joint à AnonOps, mais seulement à titre d'observateur. Alors qu'il se familiarise avec les us et coutumes du collectif, il établit des contacts avec des Anons. Le 21 juin, il se jette enfin à l'eau. Il tente d'abord d'approcher Sabu, à qui il souhaite transmettre des documents, mais en vain. Il décide donc d'envoyer des messages privés à deux autres membres de LulzSec, Topiary et tflow, dans lesquels il leur offre certains «bonbonz» qu'il a en sa possession. Le jeune homme vient d'obtenir un privilège d'accès au site web du ministère de la Sécurité publique de l'Arizona, dont il a siphonné toutes les données qu'il a pu trouver. LulzSec finit par accepter d'être dépositaire de l'information, qu'il rend publique en quatre lots sous le titre «Chinga la Migra» («Merde à la police de l'immigration» en espagnol). Elle inclut les courriels, les noms, les numéros de téléphone, les adresses personnelles et les mots de passe de policiers de l'Arizona, ainsi que des documents opérationnels comme des comptes rendus confidentiels du renseignement et des manuels.

Hammond n'aurait pu choisir meilleur moment pour agir. Lorsqu'il leur transmet ses données, ses interlocuteurs vivent un grand bouleversement: de bande de *tricksters* fabulateurs, LulzSec est en train de se muer en groupe d'activistes révolutionnaires. Ses membres ont adopté un

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

nouveau nom et un nouveau programme: AntiSec, apocope d'«Anti-Security». La transformation est difficile à expliquer. Des initiés me confirmeront que, même de leur point de vue, la période en est une de chaos: «Le chaos régnait en ce sens où d'innombrables sous-groupes se formaient, se scindaient, se redéfinissaient. [...] C'était l'époque de LulzSec, d'AntiSec, de TeaMp0isoN, de la A-Team, de CabinCr3w, des Buccaneers, des Panther Moderns, etc.», me racontera un Anon. Mystères mis à part, une chose demeure certaine: au cours de l'été 2011, Anonymous vit une véritable explosion cambrienne d'équipes de hackers. Alors que, auparavant, les scènes nord-américaine et européenne étaient dominées par un seul réseau IRC (AnonOps) et un groupe dissident (LulzSec), tout un archipel d'îlots hackers émerge soudain des eaux anonymes (AntiSec deviendra le plus visible et le plus célèbre d'entre eux).

«C'est maintenant ou jamais. Montez à bord, nous vous attendons.»

Début juin 2011, LulzSec vogue à vive allure, laissant derrière lui un sillage extravagant, au grand plaisir des autres internautes. Ses membres ne le savent pas encore, mais ils filent tout droit vers une tempête. Le 19 juin, soit quatre jours avant la divulgation de Chinga la Migra, LulzSec lance sans crier gare l'opération AntiSec. Fidèle à son habitude, le groupe annonce celle-ci en publiant un communiqué de presse sur Pastebin. Le document se distingue cependant des précédents par un élément déterminant: son ton. Ne comportant qu'une infime trace d'humour (une histoire de sang de lézard et une référence aux paroles du thème de l'émission *La croisière s'amuse*), il véhicule un discours étonnamment révolutionnaire. LulzSec y déclare aussi quelque chose qu'il n'a jamais reconnu auparavant, à savoir que l'opération est un projet d'Anonymous:

> Bienvenue dans l'opération Anti-Security (#AntiSec). Nous encourageons tout vaisseau, grand ou petit, à ouvrir le feu sur tout

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

gouvernement ou agence qui croisera son sillage. Nous approuvons sans réserve l'utilisation du mot «AntiSec» dans tout défaçage d'un site web gouvernemental ou tout graffiti.

Que vous soyez avec ou contre nous, que vous entreteniez de vieilles rancunes à notre égard ou que vous soyez animé d'un ardent désir de couler notre navire solitaire, nous vous invitons à vous joindre à la rébellion. C'est ensemble que nous pourrons nous défendre afin d'éviter que notre vie privée soit ravagée par des goinfres avides de profit. Que votre chapeau soit blanc, gris ou noir, quelle que soit la couleur de votre peau, c'est sans importance. Si vous êtes témoin de corruption, révélez-la sans attendre, au nom d'Anti-Security.

Notre priorité consiste à subtiliser et à divulguer tout renseignement d'État confidentiel, courriels et documentation inclus. Nos cibles de prédilection sont les banques et autres institutions de haut rang. Si elles tentent de freiner notre progression, nous riposterons par le feu de nos canons enduit de sang de lézard.

C'est maintenant ou jamais. Montez à bord, nous vous attendons[6].

Pourquoi Topiary, qui a rédigé le communiqué de presse, a-t-il opté pour cette prose révolutionnaire? Tous les indices convergent vers Sabu. Quelques semaines auparavant, il a réclamé à grands cris, en ligne, qu'on relance un vieux projet d'antisécurité.

Le mouvement antisécurité a connu un bref essor au tournant du siècle chez des hackers *black hats* qui méprisaient l'industrie de la sécurité informatique en général et les *white hats* en particulier. À l'époque, les hackers étaient de plus en plus nombreux à chercher du travail dans le secteur et à en trouver. Au nom de l'antisécurité, des *black hats* ont donc décidé de s'attaquer aux professionnels de la sécurité (en les doxant et en rendant public le contenu de leurs boîtes de courriels). Ils dénonçaient la pratique, de plus en plus répandue, consistant à révéler publiquement *exploits* et vulnérabilités. Un document fondateur résume leur argumentaire:

Notre mouvement a pour objectif de promouvoir une nouvelle politique d'antidivulgation dans les milieux de l'informatique et de la

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> sécurité des réseaux. Nous ne nous opposons pas à la publication de toute information relative à la sécurité informatique, mais nous souhaitons mettre un terme à la divulgation systématique de tout *exploit* ou vulnérabilité inconnus ou non encore rendus publics. En substance, une telle politique empêcherait la publication de tout document confidentiel pouvant permettre à des *skiddies* de nuire à des systèmes en appliquant des méthodes inconnues[7].

Bien que cette déclaration pût sembler mesurée, le groupe menait des actions on ne peut plus audacieuses. Un manifeste antisécurité plus récent traduit bien la pagaille que ces hackers semaient dans l'industrie de la sécurité informatique (voir l'encadré suivant). Aussi étrange que cela puisse paraître, les premiers militants antisécurité étaient entre autres motivés par la préservation de leur culture; ils souhaitaient «reprendre les devants de la scène».

Le premier mouvement antisécurité était un animal bien différent de celui qu'imaginent Sabu et Anonymous. Bien que l'AntiSec de 2011 ait peu de considération pour les *white hats* et soit dégoûté par la cupidité flagrante de l'industrie de la sécurité, ceux-ci ne sont pas ses principaux ennemis. AntiSec est plutôt motivé par un sens diffus de la justice. Son programme consiste à s'insinuer dans les systèmes des banques, des États, des firmes de sécurité et d'autres entreprises en vue d'y trouver des informations politiquement compromettantes. Et, aspect sans doute le plus important, le groupe n'entend pas agir dans la discrétion.

antisec

/Dévoilé

- **Merde à la divulgation systématique**
- **Merde à l'industrie de la sécurité**
- **Laissons les jours zéro confidentiels**
- **Hackez tous ceux que vous pouvez hacker, et plus encore**

Fondez-vous dans le décor.
Gagnez la confiance d'autrui.
Ne faites confiance à personne.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Hackez tout le monde.
Ne divulguez rien.
Détruisez tout.
Reprenez les devants de la scène.
Ne trahissez jamais vos principes, ne capitulez jamais.
Agissez dans l'anonymat, ne laissez aucune trace.

[Bonnes lectures:
Groupe Antisec dévoilé [site miroir] [site miroir] [site miroir] [site miroir] [site miroir]

[Fichiers:
Groupe Antisec fichiers [site miroir] [site miroir] [site miroir] [site miroir] [site miroir]

[Liste de contrôle/Objectifs:
Bloquer tout forum public, groupe ou site web qui fait la promotion d'*exploits* et d'outils, ou qui comporte des sections pour la frime. Envoyer les *exploits* équipés de /bin/rm aux *white hats* et les laisser rm leurs propres boîtes par eux-mêmes. Faire connaître le mouvement antisécurité.
Relancer le pr0j3t p4g4i113

[Règles d'engagement:
Éviter d'être trop sûr de soi.
Ne sous-estimer personne.

[Contact / Pour soumettre un article:

C'est sur Twitter que LulzSec mentionne AntiSec pour la première fois: «Approchez-vous! Bâtissons ensemble un nouveau cybermonde. Les cibles seront plus grosses, il y aura plus de blocages. #ANTISEC[8].»

Le 7 juin 2011 à 22 h 15, soit trois jours à peine après la publication de ce message, des policiers du Federal Bureau of Investigation (FBI) débarquent aux Jacob Riis Houses, un grand ensemble d'habitations en brique du Lower East Side de Manhattan. Ils se rendent dans ce bastion portoricain pour arrêter Hector Monsegur, dit Sabu. Selon le mandat émis pour permettre au FBI d'avoir accès au compte Facebook de Monsegur, lequel a fait l'objet d'une fuite, une entreprise hackée par Anonymous a mis la main sur une adresse IP qu'elle a transmise aux autorités. Les policiers sont parvenus à récupérer les renseignements relatifs à l'utilisateur de ladite adresse, ce qui les a menés à l'adresse postale et à l'adresse courriel du hacker. S'ils voulaient passer au crible son compte Facebook, c'était dans l'espoir d'y trouver des «images» qui leur permettraient de «confirmer

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

l'identité de l'individu qui a facilité l'intrusion non autorisée» et potentiellement d'autres pistes si le suspect avait partagé la moindre information avec ses camarades hackers par l'entremise du média social. Bien qu'il ait tout juste 27 ans, Sabu est le père adoptif des deux filles de sa tante incarcérée, lesquelles n'ont pas encore 8 ans. En plus d'avoir documenté l'activité du jeune homme au sein d'Anonymous et de LulzSec, le FBI détient des preuves qui l'associent à une fraude de cartes bancaires. Devant la perspective de passer des dizaines d'années en prison et de perdre ses deux enfants adoptifs, Sabu panique.

Quatre jours auparavant, des membres de LulzSec se sont inquiétés de voir des sympathisants quitter le navire. Sabu a alors affirmé qu'il effacerait tout son disque dur:

<Neuron> Sabu, avons-nous perdu du monde?
<storm> oui
<storm> en avons-nous perdu?
<Sabu> ouais
<storm> qui?
<Sabu> recursion et devurandom nous ont quittés respectueusement
<Sabu> en disant qu'ils n'étaient pas partants pour l'action
<Neuron> j'ai déjà commencé à effacer tout mon bureau [...]
<Sabu> ouais
<Sabu> efface tout
<Sabu> je suis en train d'effacer toute ma merde

Quoi qu'il ait fait ou non à ce moment, Sabu passe de hacker militant radical à indicateur du FBI, à qui il fournira un accès direct à LulzSec. Constamment en ligne, les membres de LulzSec trouvent louche l'absence de vingt-quatre heures de Sabu. Pour tester sa loyauté à son retour, ils lui demandent de prendre le contrôle d'un serveur. Il s'exécute aussitôt, ce qui apaise leurs craintes. Le FBI lui a bien sûr donné son aval au préalable, afin de protéger sa couverture.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Peu après son arrestation, Sabu radicalise le discours d'AntiSec, dont LulzSec avait donné un avant-goût sur Twitter. Il doit savoir que Hammond sera séduit par de tels propos. Ce dernier est sans doute déjà surveillé par le FBI, car il est un des rares anarchistes et hackers américains à avoir fait de la prison. Le changement de ton d'AntiSec reflète peut-être simplement la continuité d'un engagement sincère. On n'en aura probablement jamais le cœur net. On sait cependant que, immédiatement après avoir retourné sa veste, Sabu insiste pour que le communiqué de presse d'AntiSec soit marqué politiquement. Et que Topiary rédige celui-ci de bon gré. Dans un courriel, Topiary m'expliquera: «Sabu souhaitait vivement que j'écrive ce message, mais, élément sans doute plus important, il était impressionné par le nombre d'abonnés qu'avait alors LulzSec sur Twitter, qu'il considérait comme une plateforme où défendre de telles positions politiques. On pouvait percevoir là quelque performance artistique d'adolescents angoissés, mais d'autres observateurs prenaient évidemment la chose beaucoup plus au sérieux.»

Le public, la presse et les membres d'Anonymous ignorent alors que le FBI tient la bride haute à Sabu, mais tout le monde constate à quel point la prose s'éloigne du style habituel de LulzSec. De Fox News à *Adbusters*, les médias font écho au communiqué, que des journalistes critiquent vertement en se demandant ce qui peut bien se passer. Stephen Chapman, de *ZDNet*, pose la question centrale: «Ce qui, jusqu'ici, ne poursuivait qu'un objectif vain, constitué d'une série de cibles gratuites choisies au hasard, est en train de devenir un véritable mouvement d'opposition au gouvernement et à l'ordre établi qui pourrait prendre des proportions considérables. Après avoir été mise en scène par Hollywood pendant des années, la révolution numérique aurait-elle enfin commencé? Peut-être[9].»

Tout le monde – moi y compris – se demande alors s'il s'agit d'un nouveau tour ou de l'expression d'un véritable sentiment.

Le 20 juin, LulzSec réagit. Le groupe met à exécution la menace de l'opération AntiSec en lançant une attaque par saturation contre la Serious Organised Crime Agency du Royaume-Uni à l'aide du réseau de zombies de Ryan Cleary. Dès le lendemain, soit le 21 juin, la police arrête Cleary à

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

sa résidence du comté d'Essex, près de Londres. Les journaux de toute l'Angleterre publient des dizaines de photos du jeune homme, hacker de premier plan d'Anonymous et sympathisant de LulzSec. Le portrait qu'en brossent les médias correspond au stéréotype du jeune mâle dysfonctionnel et isolé, au corps rondelet et à la mauvaise mine. Cleary quitte rarement sa chambre, qui, même si elle n'est pas située au sous-sol, en a toutes les apparences, sa fenêtre étant bouchée par un store opaque en papier d'aluminium. Les tabloïds ne rateront aucune occasion d'exploiter le potentiel dramatique du moindre détail.

C'est dans ce contexte frénétique que Hammond contacte LulzSec en vue de lui transmettre les fichiers qu'il a subtilisés à l'État de l'Arizona. Il a d'abord voulu confier les données à Sabu, mais ce dernier s'est soudainement – et étrangement – montré sourd à ses appels. Apparemment animés du même esprit, Sabu et Hammond ont noué des liens autour de leur objectif commun d'unir les *black hats* en vue de dénoncer l'injustice et l'oppression.

Sous le pseudo d'Anarchaos, Hammond envoie donc des messages privés à Topiary et à tflow dans lesquels il insiste sur le fait qu'il n'oserait pas «toucher le serveur de torrents avec une perche de trois mètres». Avec enthousiasme, tflow accepte ses «bonbonz», que LulzSec s'empresse de mettre en ligne en les répertoriant sur les serveurs de The Pirate Bay le 23 juin. Hammond n'a pas encore gagné la confiance des membres les plus éminents de LulzSec, si bien qu'on ne l'autorise pas à se connecter aux canaux privés. Mais son hacking est le catalyseur grâce auquel la vision d'AntiSec se concrétise en action. Il écrit lui-même le communiqué de presse de Chinga la Migra:

> Nous publions aujourd'hui des centaines de comptes rendus confidentiels du renseignement, de manuels, de courriels personnels, de noms, de numéros de téléphone, d'adresses et de mots de passe de policiers de l'Arizona. Si nous prenons pour cible le ministère de la Sécurité publique de l'Arizona, c'est avant tout parce que nous nous

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> opposons au SB1070 et au profilage racial auquel se livre l'État policier anti-immigrants qu'est l'Arizona.
>
> Classés comme «sensibles», «non destinés au public» et «réservés aux autorités», les documents portent essentiellement sur la patrouille frontalière et les opérations antiterroristes, ainsi que sur le recours à des taupes pour infiltrer différents gangs, cartels, groupes de motards, groupes néonazis et mouvements contestataires.
>
> [...]
>
> Des hackers du monde entier sont en train de s'unir pour mener des actions directes contre les oppresseurs que sont les gouvernements, les entreprises, les polices et les armées du monde entier. On se revoit bientôt! ;D[10].

Peu de temps après la divulgation Chinga la Migra, Hammond, toujours en probation du fait de son opération de hacking précédente, reçoit la visite de la police de Chicago et du FBI pour un contrôle. Il trouve étrange qu'un membre du FBI accompagne l'agent de probation pour une simple vérification de routine. «Lorsqu'ils découvrent du K2 [cannabis synthétique], ils me mettent aussitôt en accusation pour possession de marijuana, ce dont je serai acquitté quand les résultats des tests arriveront», me racontera-t-il. Incarcéré pendant quelques semaines, Hammond ne sera pas témoin de la controverse suscitée au sein de LulzSec par la divulgation de ses documents. Certains membres, dont tflow, pwnsauce et, plus tard, Topiary, regrettent d'avoir rendu les données publiques. Bien que ces jeunes hommes aient déjà doxé bon nombre de dirigeants d'entreprises et publié des données tout aussi sensibles, ils ont l'impression d'avoir pris un plus grand risque en s'attaquant à des agents de police. Hammond connaît bien le territoire. Pas eux.

En fait, tflow, alors âgé de 16 ans, encourage ses coéquipiers à démanteler LulzSec. Le groupe n'existe que depuis cinquante jours, mais une telle durée représente une éternité sur internet. Étonnamment, tout le monde est d'accord, y compris Sabu. Sans avertissement, toutefois, ce dernier change d'avis. «Il était outré par notre volonté d'abandonner en

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

dépit de son opposition, m'expliquera tflow, et il obtient généralement ce qu'il veut par la manipulation.» Ryan Ackroyd (dit Kayla) me parlera aussi des stratégies de manipulation – teintées d'une grande ironie – mises en œuvre par Sabu: «Je me souviens de l'avoir entendu dire qu'il exposait ses enfants à des risques en allant aussi loin, et qu'il serait injuste d'abandonner.»

Malgré les exhortations de Sabu, c'est le camp de tflow qui finit par avoir le dessus. À la fin juin 2011, LulzSec met donc fin à ses activités. Fidèles à eux-mêmes, ses membres ne peuvent se retirer sans panache: le 25 juin, ils se livrent donc à une ultime – et colossale – divulgation, qui comprend un manuel interne de réseautique d'AOL et un demi-gigaoctet de données internes d'AT&T, ainsi que des courriels, des noms d'utilisateur et des mots de passe cryptés provenant de sites allant de HackForums.net à la librairie en ligne de l'Organisation du traité de l'Atlantique Nord (OTAN). Plus intéressante que les données elles-mêmes (du moins sous l'angle de la figure du *trickster* et de la fabrication de mythes) est la déclaration finale de LulzSec, rédigée cette fois encore par Topiary.

> Au cours des cinquante derniers jours, nous avons perturbé et exposé des entreprises, des gouvernements et même parfois la population en général, avec sans doute tout ce qui se trouve entre les trois, tout simplement parce que nous pouvions le faire. Tout cela dans le but de divertir la population, dans le désintéressement le plus total. La vanité, la célébrité, la reconnaissance sont sans importance comparées à notre désir pour ce que nous aimons tous: le frisson brut, continu et chaotique de l'anarchie. C'est là ce dont nous avons tous grand besoin, y compris les politiciens apathiques et les ratés de la vie[11].

Le communiqué de presse indique que les hackers confient les rênes de LulzSec au mouvement antisécurité (AntiSec) alors naissant. Comme me l'expliquera tflow, ceux-ci souhaitent «perpétuer héritage» de LulzSec. La déclaration finale se poursuit ainsi:

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> [...] au-delà du masque, au-delà de la folie et du désordre, nous sommes profondément attachés au mouvement AntiSec. Nous y croyons si profondément que nous lui avons redonné naissance, au grand désarroi de ceux qui voudraient plus de *lulz* anarchique. Nous espérons, nous souhaitons, voire nous réclamons, que le mouvement s'incarne dans une révolution qui pourra se poursuivre sans nous. [...] S'il vous plaît, ne baissez pas les bras. Ensemble, unis, nous pourrons écraser nos oppresseurs et nous donner le pouvoir et la liberté que nous méritons.

Incarcéré, Hammond compte les jours qui le séparent de ses retrouvailles avec sa nouvelle communauté de hackers hyperpolitisés. À sa sortie de prison, il est «prêt à reprendre du collier», comme il me le dira plus tard. Il n'a aucune peine à trouver des camarades enthousiastes.

Mais l'avenir d'AntiSec demeure incertain jusqu'à ce que trois facteurs soient réunis. Premièrement, Sabu, désormais taupe à plein temps, se donne pour mission de maintenir AntiSec à flot. Deuxièmement, Hammond est le complice idéal. Hacker talentueux, il est convaincu du bien-fondé de la mission d'AntiSec, dont il devient l'infatigable cheval de trait en finissant par y consacrer l'essentiel de son temps libre. Le troisième facteur, tout aussi fondamental, est la présence d'une équipe digne de ce nom. Certains membres de LulzSec ont fait leurs adieux définitifs, mais d'autres se sont joints au nouveau groupe. L'équipe complète d'AnonOps comptera de 8 à 12 membres actifs, dépassant ainsi l'effectif dont disposait LulzSec dans ses meilleurs jours. Constituée de hackers et d'une poignée de stratèges, elle s'est installée sur un canal secret (au nom pas si secret de #antisec) d'un serveur appelé cryto. Plusieurs de ses militants ont travaillé ensemble lors des opérations du Printemps arabe. J'en ai moi-même connu quelques-uns à l'époque, alors que je fréquentais #freedommods, un des canaux accessibles sur invitation seulement pendant ces opérations révolutionnaires.

Souvent perçu comme étant le chef d'AntiSec, Sabu n'orchestre pourtant pas les opérations ni ne donne d'ordres (en fait, il semble assez

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

éparpillé pendant cette période, même si, comme nous le verrons plus loin, il adressera certaines requêtes précises de hacking à Hammond). Les membres du noyau d'AntiSec travaillent parfois de concert, mais, en général, ils se scindent en sous-groupes menant chacun son opération. Par exemple, un canal distinct est créé pour hacker la firme de sécurité ManTech. Certaines de ces opérations autonomes n'incluront jamais Sabu, dont les contributions sont rarement d'ordre technique.

Néanmoins, Sabu joue deux rôles essentiels. Il est le principal intermédiaire pour la plupart des *exploits* et renseignements confiés à l'équipe, et il devient le visage public d'AntiSec. Alors que Topiary veillait aux relations publiques de LulzSec en *trickster*, Sabu s'occupe de celles du nouveau groupe en donnant l'image d'un porte-parole sérieux. En fait foi ce tweet publié le 20 juin, quelques semaines après son arrestation: «Opération Anti-Security: pastebin.com/9KyA0E5v. L'opération de hacking la plus importante et la mieux coordonnée de tous les temps. Toutes les tendances sont les bienvenues. Nous ne faisons qu'un.»

Quelques membres d'AntiSec exhortent Sabu à adopter un profil public distinct, individuel. Cet été-là, à la fois sous les encouragements de ses camarades et sous la pression du FBI, il utilise Twitter à plein régime en y publiant un chapelet de messages marqués par une rhétorique révolutionnaire enflammée. Usant de son charisme, il acquiert un statut digne d'une idole. La dissolution de LulzSec a marqué la disparition des *tricksters* mythiques. Et bien que quelque chose relève du mythe chez Sabu, son image publique n'a rien de celle d'un *trickster*. Il incarne plutôt l'archétype du hacker révolutionnaire et hors-la-loi. Dans les mois qui ont précédé cette période, je l'ai évité autant que possible. Toutefois, au milieu de l'été 2011, alors qu'il se hisse au premier plan, je finis par me dire qu'il est temps pour moi de le contacter.

Sabu

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Fête de l'Indépendance des États-Unis, 4 juillet 2011. À San Juan, Puerto Rico (la ville où j'ai grandi), assise dans une salle dépourvue de climatisation où règne une chaleur accablante, le front ruisselant de sueur, je peine à terminer la lecture d'une interview de Sabu[12].

Réalisée par Samantha Murphy pour le magazine *New Scientist*, l'interview est la toute première qu'ait accordée Sabu à un média. Je me sens un peu nulle, car, bien que je sois une des plus éminentes spécialistes d'Anonymous, je n'ai jamais eu la moindre conversation avec ce pilier du collectif. Pour être honnête, si j'ai gardé mes distances d'avec lui, c'est parce que je le trouve intimidant. Sabu n'est pas d'un naturel tout à fait chaleureux. Avant de retourner sa veste, il était beaucoup plus discret en ligne. Affichant une sorte d'attitude de révolutionnaire dur à cuire, il n'est pas le genre de type avec qui bavarder de tout et de rien. Lorsqu'il invite ses pairs à se soulever, il a l'habitude de les appeler «frères» et «sœurs». Lors de séances de chat sur IRC, il laisse souvent tomber le mot «nègre», et, contrairement aux trolls, il semble le faire sans la moindre pointe d'ironie. Loin de l'adolescent riche, aliéné et blanc confiné dans un sous-sol, il dégage plutôt l'aura d'un voyou endurci. Se pourrait-il que son aliénation et sa colère ne découlent pas de l'anomie de la classe moyenne, mais de la pauvreté, de la marginalisation raciale et d'une famille déchirée?

L'interview raconte une équipée de 1999 lors de laquelle Sabu a défacé des sites web pour réclamer la fin de la présence militaire des États-Unis sur la petite île portoricaine de Vieques. Ma lecture terminée, je prends mon courage à deux mains et lui envoie un message privé:

> <biella> salut Sabu, je voulais juste te féliciter pour ce que tu as fait à Vieques
> <biella> je suis originaire de la isla et j'étais pas mal engagé pour l'environnement à l'époque

L'attente de sa réponse me semble une éternité. J'ai l'impression que le temps s'est arrêté, que les gouttes de sueur se sont figées à mi-course de mon dos. Mais, en fait, il me répond presque immédiatement:

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<Sabu> super

Puis:

<Sabu> alors, c'est quoi ton but? j'ai vu ton nom associé à la police fédérale, au mouchardage ou à l'écriture de documents sur anonymous
<Sabu> dis-moi quelles sont tes véritables intentions
<Sabu> ça m'intéresse

Mes pensées tourbillonnent. Dans ce milieu où la réputation compte beaucoup, les insinuations de Sabu sont pour le moins blessantes. Je finirai par comprendre qu'elles découlent d'une tactique astucieuse: le hacker met en place un cadre dans lequel je pourrai difficilement *le* considérer comme une taupe potentielle. Il ne me viendrait alors jamais à l'esprit qu'il puisse collaborer avec le FBI. La question de savoir comment je pourrai me défendre de ses accusations prend le dessus sur toute autre considération:

<biella> je ne suis qu'une anthropologue

Une milliseconde après avoir tapé cette phrase, je réalise à quel point celle-ci peut sembler stupide. Quiconque a la moindre connaissance de l'univers des mouchards sait que la Central Intelligence Agency (CIA) a toujours compté des anthropologues parmi ses agents secrets. Je tente de restructurer mon propos:

<biella> je suis tombée sur Anonymous par hasard en 2008
<biella> par l'entremise de la Scientologie
<Sabu> ok

Cela ne semble pas lui suffire:

<biella> ma passion, c'est la politique
<biella> c'est pourquoi j'étudie la vie politique dans les médias numériques
<Sabu> je comprends ça

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Puis, je lance quelque chose qui me donnera envie de rentrer sous terre:

> <biella> en ce qui concerne Anonymous, je suis intriguée, et inquiète aussi (FBI, mon ordinateur, etc.)
> <biella> je prends des précautions avec mes données, d'ailleurs je ne recueille pas certains types de données, ce qui est frustrant, mais je ne vois pas d'autre façon de contourner le problème
> <Sabu> mais pourquoi veux-tu recueillir des données?
> <biella> ça me déprime de voir mon nom associé au mouchardage et au FBI, mais je comprends dans la mesure où ça fait partie du boulot
> <Sabu> histoire?
> <Sabu> recherche en sciences sociales?
> <biella> je dirais une combinaison des deux

Je lui explique que mon but ne consiste pas à découvrir des «crimes», que je cherche plutôt à mieux comprendre la dynamique sociale. Notre première conversation ne se sera pas très bien déroulée. Toutefois, à ma grande surprise (et à mon grand soulagement), nos échanges par chat deviennent de plus en plus réguliers et amicaux. Je me dis que soit je l'ai convaincu de la noblesse de mes intentions, soit il s'est renseigné sur moi auprès d'autres membres d'AnonOps. À ce moment-là, je suis convaincue que des taupes sont infiltrées dans le groupe, mais, en juin et en juillet, très rares sont les rumeurs qui visent Sabu, alors que d'autres membres d'Anonymous font souvent l'objet d'allégations. Mes discussions avec Sabu ne font qu'alimenter ma paranoïa. Le 23 juillet, il me demande:

> <Sabu> tu es au cœur des canaux et des comm d'anonymous
> <Sabu> tu ne reçois jamais de visites de la police fédérale?
> <biella> pas encore
> <biella> on ne m'a jamais interceptée à la frontière, même si je voyage sans mon ordinateur principal ou sans ordinateur du tout – non que j'aie en ma possession quoi que ce soit d'incriminant…

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> <biella> mais ça m'inquiète, j'ai des contacts avec l'EFF [Electronic Frontier Foundation]

Un peu comme lors de notre première conversation, où j'ai couvert Sabu d'éloges dans l'espoir de le faire parler, il se met à tenir des propos flatteurs à mon égard, et même à me remercier:

> <Sabu> pour tout le travail que tu fais
> <Sabu> en serio mucho respeto [sérieusement, mes plus grands respects]
> <Sabu> au bout du compte, le mouvement sera formidable

Il commence aussi à laisser entendre que le FBI me surveille:

> <Sabu> ce n'est pas parce que tu es réglo qu'ils ne te surveillent pas

Sabu est futé: le problème potentiel, c'est *moi*, *pas lui*. Il me le rappellera à maintes reprises tout en continuant à user de son langage révolutionnaire. Il m'est difficile de le percevoir autrement que comme un activiste passionné et fidèle à la cause.

Les joies du secret

Quelques semaines après mon premier échange avec Sabu, on m'invite à me connecter à un canal IRC secret pour une séance de chat ponctuelle entre membres d'AntiSec. Y participent une poignée d'opérateurs IRC d'AnonOps et Emmanuel Goldstein, éditeur du fanzine hacker *2600* et animateur d'une émission de radio intitulée *Off the Hook*. La discussion a pour but d'évaluer l'intérêt de Goldstein à donner son appui à Voice, un projet parallèle d'AntiSec qui tourne autour de la propagande et de la création artistique. Me voici donc introduite dans le Saint des saints. J'y observe attentivement le groupe d'une vingtaine de personnes débattre des avantages de l'action directe et de la raison d'être du projet Voice.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Sabu a établi l'ordre du jour: «Messieurs, nous allons faire appel à Emmanuel. Il sera la voix d'Anonymous et d'AntiSec à la radio, et il souhaite vivement promouvoir #voice.» Il s'avère que Goldstein n'a pris aucun engagement du genre. Et, si des Anons se disent ouverts à sa participation, d'autres manifestent immédiatement leur opposition. Certains l'accusent même d'être une taupe. Il faut savoir que les rumeurs de mouchardage font partie du décor quotidien des hackers, et que ce décor est lui-même un des principaux obstacles à la vérification du bien-fondé de ces accusations. Au fil de la discussion, un des opposants rappelle que «*2600* a souvent condamné les attaques, dont celles qu'Anonymous a menées contre MasterCard et d'autres organisations pour défendre WikiLeaks».

Adrian Lamo, le hacker qui a mouchardé Chelsea Manning, a déjà frayé avec *2600*; il avait même accès au serveur de messagerie de l'organisme. Selon certains, son exclusion n'a pas été assez stricte, et il est scandaleux que le forum Hackers on Planet Earth (HOPE), organisé par Goldstein et une vaste équipe, l'ait inclus parmi ses panélistes.

Je suis particulièrement intriguée par les propos d'un participant à la discussion appelé Anarchaos. Je ne l'ai jamais vu en ligne auparavant, et je n'aurai pas l'occasion d'avoir une première conversation avec lui (sous un autre pseudo) avant quelques mois. Alors que Goldstein émet des doutes quant à la pertinence de tactiques comme l'attaque par saturation et la mise en place de Black Blocs dans les manifestations de rue, Anarchaos défend leur légitimité avec conviction. «J'ai des raisons personnelles et politiques de mener des actions directes contre les forces qui nous oppriment, affirme-t-il. N'allez pas croire que les gens qui luttent avec acharnement ne se servent pas de leur tête.» Des Anons abondent dans le même sens: «Nous sommes tout à fait capables de mener des attaques plus raffinées, mais, quand nous sommes dans les tranchées et que nous ouvrons le feu sur nos ennemis, nous ne voulons pas voir d'autres prétendus hackers miner nos efforts.» Par la suite, quelqu'un ajoute que «la diversité des tactiques est la meilleure façon d'obtenir gain de cause dans une lutte».

Ce qui a commencé comme un débat fascinant sur la diversité des tactiques dégénère rapidement en foire d'empoigne. À un certain moment,

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

quelqu'un demande à Goldstein s'il m'a déjà rencontrée (il ne l'a jamais fait). L'attention venant de se tourner vers moi, j'en profite pour lui donner mon opinion sur le panel de HOPE auquel Lamo a participé, à savoir que j'ai trouvé l'exercice «époustouflant» et que je suis «très heureuse que vous l'ayez organisé».

«Vous ne pouvez pas imaginer la pression que j'ai subie pour NE PAS le faire», répond Goldstein. Des participants en profitent pour dire qu'ils n'ont pas encore décoléré: «Lamo devrait être banni de tout rassemblement de hackers; pour bien des gens, c'était un autre clou dans le cercueil de *2600*, qu'ils finissent par considérer comme un repaire de traîtres.»

La discussion se recentre brièvement sur la possibilité que *2600* contribue au projet Voice, puis tourne à nouveau au vinaigre. Goldstein décide de partir: «Je suis désolé de susciter tant d'animosité, alors je m'en vais. Mais nous restons ouverts au dialogue.» Le projet Voice sera lancé peu de temps après sur un canal IRC public, sans l'aide de Goldstein. Bien que la séance de chat n'ait pas rempli son objectif, elle a confirmé ce dont je me doutais: que l'équipe d'AntiSec compte un certain nombre de hackers actifs, mais cachés, dont Anarchaos. Qui sont ces gens? Pourquoi ne les ai-je jamais vus auparavant? Le noyau de LulzSec, dont faisaient partie Topiary, tflow et Sabu, était surtout constitué de personnalités connues. Déjà si difficile à saisir, Anonymous est désormais nimbé d'un mystère encore plus opaque.

Et je suis moi-même de plus en plus attirée dans l'orbite du secret. Jusqu'ici, j'ai tenté de garder mes distances avec les canaux où l'on organise des actions illégales. Quand je discutais en privé avec des Anons, je leur demandais régulièrement d'éviter de me confier des détails incriminants (sachant qu'ils devaient mourir d'envie de se vanter d'avoir vaillamment compromis quelque système de sécurité). J'ai expliqué à tout le monde que ma fonction d'anthropologue implique souvent de prendre des notes, d'enregistrer des segments de journaux et de recueillir des données. Même si mes données sont cryptées, je ne dispose d'aucun privilège qui puisse m'éviter d'être considérée comme la complice d'un crime. Par conséquent, on ne m'invitait pas sur les canaux secrets et

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

j'évitais (la plupart du temps) de lire les fanfaronnades sur les opérations de hacking illégales. Je fais preuve de franchise, ce qui, je crois, a permis aux Anons de mieux comprendre ce à quoi je suis occupée – chose rare dans cette culture de la méfiance, de la suspicion, des rumeurs et de la peur. Avec AntiSec, j'ai l'impression que la situation n'est plus la même. Je suis en train de m'enfoncer dans les recoins les plus profonds et les plus sombres du labyrinthe, on me permet de jeter un coup d'œil à des conversations privées, et je crains de plus en plus que les choses tournent mal.

«Se regrouper avec d'autres personnes cultivant la même pensée en de petites cellules tournées vers un but précis constitue, pour la grande majorité des hommes et des femmes, une source de profonde satisfaction psychologique. Le sentiment de la singularité ajoutera au plaisir d'être plusieurs, mais plusieurs formant un tout, et celui du secret pourra intensifier ce plaisir, presque jusqu'à l'extase», écrivait Aldous Huxley[13]. Pour les hackers d'Anonymous, le secret est assurément une importante source de motivation. Il fait en quelque sorte partie des moyens de subsistance de cette communauté marginale. Et, bien qu'«extase» soit un terme un peu trop fort dans mon cas, je ne peux nier que mon admission dans ce cercle d'initiés m'ait procuré une certaine euphorie.

Anonymous, où es-tu?

J'ai d'abord trouvé enivrant d'être tapie dans l'ombre avec Anonymous, mais, au début du mois d'août 2011, mon humeur a commencé à tourner au vinaigre. Le caractère purement militant des opérations a fait évoluer l'activité frénétique du collectif vers quelque chose d'inédit. Je me demande à quel moment le FBI ou une autre agence de l'État pincera d'autres Anons, voire me rendra visite. À l'instar de LulzSec, AntiSec mène des opérations de hacking presque sans interruption et leur donne des titres sarcastiques qui ne semblent viser qu'à pousser l'État à réagir: #FuckFBIFridays (les vendredis «merde au FBI»), #ShootingSherrifsSaturday (les samedis où

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

l’on tire sur les shérifs), #MilitaryMeltdownMonday (les lundis où l’on fait craquer les militaires).

AntiSec doxe des bureaux de shérifs, défface et anéantit des sites web associés à la police comme celui de la California Statewide Law Enforcement Association, et divulgue des renseignements personnels sur les chefs de police new-yorkais. En juillet seulement, ses membres attaquent les sites web de 77 organismes chargés de l’application de la loi (tous hébergés sur le même serveur). Ils rendent public le gigaoctet de données de la société Vanguard Defense Industries qu’ils ont subtilisé en hackant le compte de courriel d’un de ses vice-présidents. Ils révèlent à la face du monde les documents qu’ils se sont «procurés», dont une proposition du sous-traitant militaire IRC Federal au FBI; intitulée «Special Identities Modernization (SIM) Project», celle-ci vise à identifier les personnes qui «pourraient» représenter un risque criminel ou terroriste dans l’avenir. Ils affirment avoir infiltré divers réseaux internes du département de l’Énergie des États-Unis et y avoir envoyé des messages pressant ses fonctionnaires de se retourner contre l’État au lieu de travailler à son service. Ils hackent le sous-traitant fédéral ManTech International, dont ils rendent publics près de 400 mégaoctets de données faisant état de ses négociations avec l’OTAN et l’armée de terre des États-Unis (sans parler des courriels des employés). Ils s’en prennent au gros sous-traitant en sécurité Booz Allen Hamilton; bien qu’incapables de mettre la main sur des documents officiels (un de ses employés d’alors, Edward Snowden, finira par y arriver), ils parviennent à subtiliser 90 000 courriels militaires qu’ils téléchargent aussitôt sur The Pirate Bay avec une longue analyse faisant état d’«informations stratégiques» sur l’entreprise, dont la ventilation de ses sources de revenus. Les choses ont pris un tour très sérieux.

Au cours de ce regain d’activité, les arrestations se succèdent. En juillet, 14 Américains sont arrêtés pour avoir participé aux attaques par saturation contre PayPal, et les autorités britanniques appréhendent deux membres de LulzSec, soit Topiary en Écosse et tflow à Londres (le véritable nom de tflow n’est pas rendu public parce que le prévenu est mineur). Juste

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

avant son arrestation, Topiary a laissé cet adage sur son compte Twitter: «On ne peut pas arrêter une idée[14].»

C'est un été chaud. Ce climat menaçant me fait faire des cauchemars dans lesquels des agents de la police fédérale cognent à ma porte. Je me demande dans quelle galère je me suis embarquée, et je ne suis pas la seule. Lors d'une interview, un Anon me fait part de sa surprise: «Aucun de nous ne s'attendait à ça. [...] Emprisonnés pour des décennies, en cavale, en exil... Suicides, maladie mentale, TSPT[15], etc.» De plus en plus d'Anons me confient qu'ils ont peur, ce qui alimente mon malaise. Le 1er août, quelqu'un m'écrit que «ça devient EXTRÊMEMENT dangereux en ce moment [...] pour ceux qui font partie d'AntiSec, par exemple». Le lendemain, un autre hacker raconte: «Un hélicoptère a atterri dans le champ voisin de chez moi à sept heures ce matin. Mon rythme cardiaque a dû grimper à 200, jusqu'à ce que je réalise qu'il faisait de la pulvérisation agricole.» Face à tous ces gens qui me confient leurs sentiments de panique, à la série d'arrestations, au fait que je n'ai plus de vie parce que je consacre tout mon temps à cette recherche, à des interactions sous pseudonymes se déroulant essentiellement par écrit, et devant l'emprise croissante du secret, je suis de plus en plus contrariée et épuisée. Tout ça me tourmente. Je m'inquiète de l'avenir d'Anonymous, de mon avenir à moi et du sort des arrêtés. Des membres d'AntiSec en viennent à remarquer que je suis déprimée. Certains me contactent en privé pour m'encourager à ne pas abandonner. L'un d'eux me dit que, si je m'en vais, je risque de manquer «des choses qui sortent de l'ordinaire».

Je n'ose pas lui demander de quoi il pourrait bien s'agir. Les divulgations et les perturbations continuent d'aller bon train, mais elles n'ont plus le lustre qu'elles avaient auparavant. À mes yeux, #FuckFBIFridays et #MilitaryMeltdownMonday commencent à ressembler à #FuckFBIFatigue (l'épuisement d'«emmerder le FBI») et à #MyMeltdownMondays (les lundis je craque). Aussi, même si AntiSec m'a ouvert ses portes, une activité croissante semble émaner d'autres petites équipes de hackers dont j'ignore à peu près tout, ce qui m'irrite. L'ère des soulèvements à grande échelle d'Anonymous semble révolue. Si le collectif

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

a suscité mon enthousiasme, c'est pour une raison bien précise: il s'agit du plus vaste mouvement de contestation populaire de l'histoire d'internet. J'ai soudain l'impression qu'AnonOps et Anonymous sont en train de revenir à une forme plus classique d'avant-gardisme hacker. Sous un angle strictement logistique, cela signifie qu'Anonymous devient encore plus difficile à étudier.

Avec le recul, on peut trouver au moins une raison concrète à la fragmentation croissante d'Anonymous: l'interférence directe de l'État. Grâce aux documents divulgués par Edward Snowden en 2013, on sait désormais que, au cours de l'été 2011, le Government Communications Headquarters (GCHQ, quartier général des communications du gouvernement britannique) a ciblé les infrastructures de communication du collectif. Une unité spéciale du GCHQ, le Joint Threat Research Intelligence Group (JRIG, groupe mixte du renseignement pour la recherche sur les menaces), qui pratique aussi l'intrusion à la façon du Counter Intelligence Program (COINTELPRO), a lancé des attaques par saturation contre Anonymous, les opérations Wealth (fortune) et Rolling Thunder (coup de tonnerre)[16].

Il s'agit du premier exemple connu d'un État occidental qui utilise secrètement l'attaque informatique par saturation (un crime au Royaume-Uni et aux États-Unis) comme tactique contre ses propres citoyens. Le GCHQ a qualifié l'opération de réussite; selon les diapositives rendues publiques, cette attaque contre l'IRC d'AnonOps a fait en sorte qu'«un mois plus tard, 80 % des participants ne fréquentaient plus les canaux IRC». À ce moment-là, des Anons britanniques s'étaient déjà fait arrêter pour avoir fait la même chose. L'un d'eux, Chris Weatherhead, dit Nerdo, était un opérateur d'AnonOps important et très apprécié. Il a fini par être condamné à dix-huit mois de prison pour son rôle dans les attaques par saturation menées dans le cadre des opérations Avenge Assange et Payback. On ne l'a pas jugé coupable d'avoir mené concrètement une attaque, mais plutôt d'avoir contribué aux opérations en administrant le serveur IRC. L'État britannique, en revanche, n'a subi aucune sanction pour ses attaques par saturation contre les activistes. Manifestement, la loi n'a pas été

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

appliquée équitablement. «Mon gouvernement a lancé une attaque par saturation contre des serveurs qui m'appartenaient, puis m'a jugé pour avoir mené des attaques par saturation. Sérieusement, c'est quoi cette merde?» a lancé Weatherhead sur Twitter[17].

En rendant justice de cette façon pour le moins brutale, on punit des milliers de citoyens engagés pour la seule raison qu'une poignée de leurs semblables ont commis des actes de vandalisme numérique.

Si cette tentative de dissuasion a paralysé Anonymous en général, elle n'empêche pas AntiSec de poursuivre ses activités. Le groupe fréquente un autre réseau IRC. Bien que certains de ses membres se soient fait arrêter et que d'autres aient abandonné le navire pour diverses raisons, il règne un consensus selon lequel «il est impossible de revenir en arrière», m'explique un Anon.

Quant à moi, je dois prendre une pause. Je décide donc de me rendre en Allemagne pour assister à un des forums de hackers les plus fameux de la planète, The Chaos Communication Camp, organisé tous les quatre ans par le Chaos Computer Club. Je me dis qu'un moment hors ligne en compagnie de hackers que je connais, d'amis, ou à tout le moins de personnes rencontrées en chair et en os, pourrait atténuer l'espèce de vertige que je ressens toujours.

Après quelques jours et nuits au festival de hackers, et un vol de retour matinal, je rentre aux États-Unis plus épuisée encore que je ne l'étais avant de partir. Anonymous, en revanche, semble dans un meilleur état d'esprit. En me frayant un chemin dans l'aire de récupération des bagages, j'aperçois au loin, sur un écran de télé, un visage familier: le masque de Guy Fawkes. Troublée, je me précipite vers le moniteur, syntonisé sur CNN. On y montre un tweet appelant au déclenchement de l'opération BART (voir ici). Des indices visuels me permettent de constater qu'il ne s'agit pas seulement d'une opération d'envergure. Celle-ci semble aussi s'inscrire dans la tumultueuse tradition des grands soulèvements de l'Anonymous de la vieille école. Les participants que le GCHQ prétendait avoir éradiqués à 80 % en menant son attaque par saturation étaient de retour, accompagnés de centaines de nouveaux venus.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

L’opération BART découle d’un événement survenu le 3 juillet 2011: l’homicide par arme à feu de Charles Hill par la police du métro à la station Civic Center de San Francisco. Bien que l’homme fût drogué et armé d’un couteau, bien des gens considèrent que sa mort est attribuable à un usage excessif de la force. L’affaire souligne une fois de plus le problème plus large de la brutalité policière. En 2009, à la station de métro Fruitvale d’Oakland, des policiers avaient tué l’Afro-Américain Oscar Grant III en lui tirant dans le dos alors qu’ils le retenaient au sol. En réaction à l’homicide de Hill, des militants locaux ont organisé une manifestation à la station Civic Center, à laquelle une centaine de personnes ont pris part, perturbant le service de métro. Un mois plus tard, les organisateurs ont convoqué une seconde manifestation au même endroit, mais les autorités du Bay Area Rapid Transit (BART) ont décidé d’interrompre le service de téléphonie mobile sur les quais de certaines stations en vue d’empêcher la tenue de l’événement. Sur les ondes de CNN, le porte-parole de la société de transport, Linton Johnson, a justifié la mesure de cette façon: «Les manifestants nous ont contraints à prendre une décision déchirante. [...] Nous avons dû trancher entre la possibilité pour les usagers d’utiliser leur téléphone portable [et] leur droit constitutionnel de se rendre du point A au point B[18].»

Selon mes plus récentes vérifications, la Constitution des États-Unis protège tant la liberté d’expression que la liberté d’association, mais elle est muette à propos de la liberté de transport. Au courant de leurs droits constitutionnels, les geeks d’Anonymous sont évidemment outrés par la déclaration de Johnson. Le principal responsable du compte Twitter @Your AnonNews, Jackal, lance publiquement le mot-clic #OPBART avec une série de messages cinglants. Il a déjà 300 000 abonnés. Peu après la diffusion du reportage de CNN, il en attire 200 000 autres (ce qui lui vaut une visite du FBI). Les Anons et d’autres citoyens inquiets créent le mot-clic #MuBARTec pour faire le lien entre cet acte de censure et le blocage total des communications imposé par l’ancien président égyptien Hosni Moubarak quelques mois auparavant, en janvier 2011.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Jackal travaille avec un petit groupe. Il administre un canal IRC semi-privé qu'il appelle «*the cabin*» (la cabane). D'abord fréquenté par quatre personnes et conçu comme un espace social, le canal voit son nom augmenté du suffixe «Cr3w» (3quipage) à l'initiative d'un de ses membres, qui se moque ainsi gentiment de LulzSec et des autres «équipages» autoproclamés qui foisonnent alors. Au cours de l'opération BART – sa toute première –, CabinCr3w connaîtra une mutation imprévue en passant d'un canal strictement social à une équipe prolifique et fonctionnelle. Au bout de quelques mois, le groupe comptera une vingtaine de membres. Ceux-ci se feront connaître en tant que spécialistes de l'exploration de données ouvertes, qui consiste à fouiner dans des bases de données fournies par d'autres hackers ayant infiltré des serveurs à la recherche d'informations (bien que certains membres de CabinCr3w, tels Kahuna [John Anthony Borell III] et w0rmer [Higinio O. Ochoa III], qui commettent aussi des entrées par effraction numériques, finiront par se faire arrêter).

Mais à la mi-août, alors que l'opération BART ne fait que commencer, l'équipe est encore minuscule. Avec une force de travail aussi limitée, ses membres ne dorment guère au cours des trois premiers jours. Par l'entremise de Facebook, CabinCr3w communique avec les citoyens de la région pour organiser des manifestations et s'unit avec la communauté élargie des Anons en contactant certains de ses organisateurs chevronnés. Sur le serveur AnonOps, le canal public #opbart devient un point de ralliement. Tout le monde s'active à la conception du matériel destiné à annoncer la manifestation prévue pour le lundi 15 août. S'inspirant des méthodes de l'opération Avenge Assange, les organisateurs jouent le rôle de chorégraphes (pour emprunter à Paolo Gerbaudo son terme si juste[19]) guidant une vague d'indignation.

Parallèlement aux manifestations et à la diffusion d'information, des participants mènent des actions plutôt risquées, bien qu'ils le fassent délibérément pour le *lulz*. Ce sont ces gestes qui attirent l'attention des grands médias. (Souvenons-nous par exemple du cliché osé de Linton Johnson publié avec un commentaire effronté, voir p. 16.)

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Mais, par-dessus tout, c'est une série d'opérations de hacking qui suscite l'intérêt des grands médias de partout aux États-Unis, de CNN à *Democracy Now!*

Le 14 août, les hackers défacent le site web myBART.org avec une image de Guy Fawkes. Peu après, une intrusion débouche sur la divulgation des données personnelles de 2 500 usagers du métro. Le 17 août, soit le lendemain de la deuxième manifestation organisée à la station Civic Center par Anonymous et des militants du coin, des hackers s'insinuent cette fois dans le site web du syndicat des policiers du BART et publient sur Pastebin les adresses personnelles, les adresses courriel et les mots de passe de 102 agents et d'autres employés de la société de transport.

Le jour même où je rentre d'Allemagne, des représentants de *Democracy Now!* m'invitent à me joindre à eux pour parler de l'opération BART à la télévision. Je frémis à l'idée qu'on me pose une question sur les grossières violations de la vie privée que constituent ces opérations de hacking et sur les contorsions nécessaires pour expliquer le recours à de telles tactiques par un collectif qui affirme se battre bec et ongles pour la protection de la vie privée. Fort heureusement, l'Anon Commander X fait aussi partie des invités de l'émission présentée en direct, et c'est à lui qu'on demande une justification:

> AMY GOODMAN: Et qu'avez-vous à dire... sur le fait de s'en prendre aux passagers eux-mêmes, à des gens qui ne souhaitent sans doute pas voir leurs données privées diffusées?
>
> COMMANDER X: En agissant autrement, comment pourrait-on amener le monde à réagir et assurer la sécurité de l'information? Comment pourrait-on amener ces entreprises et ces gros États à protéger les renseignements qu'on leur confie? Je crois que notre message est passé, et je vous parie qu'ils vont corriger la situation[20].

Commander X, dont la voix a été modifiée, n'est pas l'auteur de l'intrusion. Le présumé responsable de celle-ci partage cependant son avis, de même qu'une minorité d'Anons. À ce moment-là, j'ignore qui est derrière ces

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

opérations de hacking, et je ne sais quelle est l'opinion des autres Anons sur la question. En arrivant chez moi à la suite de l'émission, j'aurai tôt fait d'en savoir plus.

Bien que l'immense majorité (voire la totalité) des Anons s'entendent sur la nécessité de dénoncer publiquement la censure imposée par le BART, l'opération de hacking et le *doxing* de la clientèle sont loin de faire l'unanimité. Jamais je n'ai été témoin de plus fortes dissensions internes. Sur les canaux – et même en public sur Twitter –, les critiques fusent.

Prenons l'exemple de ce qui se produit lorsque, le 17 août, Lamaline_5mg se connecte au canal #opbart, revendique l'attaque contre le site du syndicat des policiers du BART et publie un lien vers les données divulguées:

<Lamaline_5mg> Salut la compagnie
<CrappyTIres> Salut Lamaline_5mg
<Lamaline_5mg> J'ai fait une petite contribution
<Lamaline_5mg> http://pastebin.com/XX7DJBqw
<Lamaline_5mg> Une fuite de http://bartpoa.com/ [site du syndicat des policiers du BART]
<Lamaline_5mg> Bonne lecture! Et partagez.
<CrappyTIres> hum
*CrappyTIres n'aime pas les fuites d'info
<OpNoPro> ces noms ont-ils déjà été diffusés auparavant?
<Lamaline_5mg> Quoi?
<Lamaline_5mg> Je sais pas. J'imagine que non.
<OpNoPro> Tu as publié des noms et des mots de passe
<OpNoPro> Nous menons une opération très clean ici
<OpNoPro> Les trucs de ce genre ne nous intéressent pas
<OpNoPro> SVP évitez de divulguer les données privées de qui que ce soit, où que ce soit, au nom d'anonymous... on ne souhaite pas balancer la vie privée de qui que ce soit... tout le monde y a droit au même titre que vous

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Tout le monde ne partage pas l'avis d'OpNoPro. D'autres Anons défendent haut et fort les méthodes *black hats* d'AnonOps:

> <sharpie> c'est sa divulgation
> <OpNoPro> Faites vos affaires en privé, personne n'a besoin d'être au courant
> <sharpie> ta gueule [...]
> <Lamaline_5mg> C'est pas ma faute si leur sécurité est pourrie
> <OpNoPro> Hé, relax
> <OpNoPro> Ce n'est pas discutable
> <OpNoPro> Chaque chose doit être laissée à sa place
> <sharpie> les gens trouvent cet irc digne d'un club de tricot de paroisse
> <OpNoPro> SVP essayez de comprendre la situation
> <sharpie> ouais
> <sharpie> je la comprends
> <sharpie> et pas mal plus que toi
> <OpNoPro> Il y a plusieurs canaux sur cet IRC
> *CrappyTIres cherche le club de tricot
> <OpNoPro> Allez-y mollo
> <OpNoPro> Réveillez-vous
> <OpNoPro> Laissez chaque chose à sa place [...]
> <sharpie> garde ta merde de moralfag white hat pour toi
> <OpNoPro> Et si jamais tu me vois dans un club de tricot, ça ira dans ta gueule
> <OpNoPro> Tu ne sais rien de mes principes moraux

Sharpie conclut en faisant écho à une des justifications les plus couramment invoquées:

> <sharpie> quelle publicité crois-tu que #opbart aurait obtenue si ces données n'avaient pas été balancées?

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Lamaline_5mg indique ensuite qu'elle n'est pas membre d'Anonymous, soulevant ainsi la question ontologique de savoir en vertu de quels critères une personne peut être considérée comme un Anon. Elle a débarqué sur le serveur IRC d'Anonymous, a offert aux participants les données personnelles qu'elle avait subtilisées puis a rédigé un communiqué de presse en collaboration avec des Anons. Si cela ne fait pas d'elle une Anon, qu'est-ce qui le ferait? Quoi qu'il en soit, le titre importe peu en regard des questions éthiques plus générales qui entourent le hacking et le *doxing*. Avec AntiSec, ces méthodes ont fini par faire partie du décor d'Anonymous, ce qui ne les empêche pas d'être de plus en plus controversées:

> <Lamaline_5mg> C'est pas anonymous
> <Lamaline_5mg> Allez vous faire foutre
> <w> OpNoPro, que ça te plaise ou non, le chaos fractal et la diversité des tactiques alimentent la révolution mondiale
> <AlbaandOmegle> Anonymous est un fouteur de merde
> <AlbaandOmegle> parce que ça marche
> <OpNoPro> balancez vos données ailleurs
> <w> OpNoPro, tu ne peux pas empêcher les gens de se servir du nom d'une opération pour doxer, lancer des attaques par saturation et hacker
> <w> OpNoPro, même si c'était ce qu'il fallait faire, tu peux tout simplement pas le faire
> <Lamaline_5mg> J'utilise pas le nom de l'opération

En d'autres recoins d'internet, ce débat se répétera sous diverses formes une bonne dizaine de fois dans les jours qui suivront. J'en conclus que la plupart des membres d'AnonOps s'opposent aux divulgations portant atteinte à la vie privée, mais appuient les autres tactiques illégales tels le défaçage du site web du BART, l'envoi massif de courriels et de fax et l'attaque informatique par saturation (peu importe que celle-ci ait échoué: le BART avait mis en place des mesures de protection efficaces). Une minorité

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

d'Anons appuie le *doxing* tout simplement parce qu'il contribue à attirer l'attention des médias, une nécessité fondamentale. Ou parce qu'il offre un parfait exemple du «chaos fractal» qui définit en partie Anonymous.

Par ailleurs, dans la foulée de cette histoire de *doxing*, des soupçons d'«opération sous faux pavillon» font rage pour la première fois au sein d'Anonymous. Une opération sous faux pavillon consiste en une intervention secrète où une agence de l'État mène une action en se faisant passer pour un groupe politique dans le but de semer la méfiance et la discorde ou de justifier l'adoption de mesures répressives par le gouvernement.

Deux jours plus tard, Lamaline_5mg publie sur Pastebin une déclaration qui semble couper court aux rumeurs de faux pavillon, sans toutefois mettre fin à la controverse:

> À mon avis, les médias devraient avoir honte de ne pas avoir condamné ces mesures draconiennes prises à l'encontre d'une manifestation visant à dénoncer l'*assassinat* d'un citoyen innocent. Il n'a pas été jugé coupable. À moins qu'on juge les gens lors de leurs funérailles? En sous-entendant que le type a eu des funérailles adéquates.
>
> Je déplore tout aussi vivement que les médias de la région de la baie de San Francisco aient défendu avec un tel acharnement le droit à l'anonymat des policiers du BART alors qu'ils n'ont manifesté aucune empathie à l'égard de l'homme abattu.
>
> Ont-ils condamné l'assassinat de cet homme?
>
> Tout ce que j'ai fait aux policiers c'est leur faire goûter leur propre médecine, c'est-à-dire le «Lamaline», un analgésique (anal)... (Allez voir.)[21]

Dans une interview qu'elle accordera ultérieurement à l'hebdomadaire *SF Weekly*, Lamaline_5mg prétendra être française et pré-adolescente (bien qu'il soit peu probable que ce pseudo désigne une femme et une personne si jeune). Elle affirmera que le hacking du BART était sa première intrusion.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Alors que l'affaire bat son plein, un message publié sur Pastebin et intitulé «Anonymous n'est pas unanime» attire l'attention de nombreux participants:

> Anonymous a un problème de perception. La plupart des gens pensent que nous sommes un groupe de hackers de l'ombre. C'est une erreur fondamentale. Anonymous est constitué de *groupes* de hackers de l'ombre, et là réside le problème. Anonymous a fait beaucoup de bonnes choses au cours des neuf derniers mois. Il a aidé d'autres groupes en soutenant des gens sur le terrain dans des pays où le mot «démocratie» est tabou.
>
> Les grands médias doivent comprendre qu'Anonymous n'est pas unanime. À ma connaissance, aucun reportage n'a encore fait cette nuance. Une minorité destructrice recueille l'essentiel de la couverture médiatique, alors que ceux qui, parmi nous, travaillent dans l'ombre en faisant du bon boulot pour les gens de chez nous et d'ailleurs n'obtiennent aucune reconnaissance[22].

Cette déclaration rend bien compte de l'importance accordée par Anonymous à la différence, à la pluralité et à la dissension, ce qui se rapproche des thèses de la philosophe politique Chantal Mouffe, fondées sur une reconnaissance de l'antagonisme[23].

Il arrive souvent aux Anons d'être en désaccord et de se livrer à de virulentes guerres de mots. Mais ils consacrent très peu d'énergie à tenter de résoudre leurs divergences ou à chercher quelque «troisième voie». Au contraire, les désaccords s'expriment haut et fort; on les écoute, on y réagit et on les accepte, non sans réticences. La plupart des Anons reconnaissent qu'aucune mesure radicale ne peut venir à bout de l'antagonisme. Ils vont de l'avant avec leurs interventions et, si une divergence s'avère insurmontable, le groupe dissident crée un nouveau noyau.

Merde à AntiSec

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

La polémique entourant les actions de hacking menées dans le cadre de l'opération BART finit par s'atténuer. Mais une autre controverse continue de faire rage. Au fil des semaines puis des mois, les critiques des interventions d'AntiSec se font de plus en plus cinglantes, même si le groupe rallie de plus en plus de sympathisants. Certains Anons considèrent que ses membres se moquent des conséquences de leurs actes, et nombreux sont ceux qui doutent de la noblesse de leurs intentions. Des rumeurs d'opération sous faux pavillon se propagent, et elles ne touchent plus simplement une action en particulier, mais bien AntiSec comme tel.

Comme il fallait sans doute s'y attendre, AntiSec est à la fois respecté, toléré et diabolisé. Par le passé, bon nombre de ses membres les plus actifs ont joué un rôle essentiel dans la constellation Anonymous-AnonOps-LulzSec. Son essor coïncide avec le déclin relatif de WikiLeaks, affaibli par des frictions internes et des ennuis judiciaires. On espère qu'AntiSec ira plus loin, qu'il affrontera de façon plus directe les détenteurs du pouvoir que sont les entreprises et les gouvernements, non seulement en donnant des spectacles éphémères comme les attaques par saturation, mais aussi en se faisant lanceur d'alerte, en dénichant et en rendant publiques des preuves infaillibles de méfaits.

Cependant, malgré un hacking incessant à la fin de l'été et au début de l'automne 2011, AntiSec ne découvre pas grand-chose. (Si Sabu n'était pas une taupe, le groupe serait sans doute plus prolifique: grâce à Monsegur, le FBI informe certaines entreprises des brèches de sécurité repérées par le groupe; celles-ci s'empressent ensuite de les colmater, verrouillant ainsi des portes qu'AntiSec vient tout juste d'entrouvrir.) En août, un Anon très présent depuis l'automne précédent quitte le groupe, écœuré. LulzSec a divulgué des données en abondance (noms d'utilisateurs, adresses courriel, mots de passe, courriels et autres documents), mais, contrairement à AntiSec, n'a jamais prétendu le faire pour des raisons politiques. Pourtant, AntiSec trouve le moyen de rester sous les feux de la rampe. Le groupe suscite ainsi le ressentiment de beaucoup d'Anons appartenant à de petites équipes qui s'activent dans l'ombre. On évoque la possibilité qu'AntiSec

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

soit devenu contre-productif et draine attention, énergie et ressources dans de vaines entreprises. «Nous étions exaspérés par le fait qu'AntiSec nous avait été imposé sans préavis. Sa création avait été planifiée de longue date; des gens d'ici y ont été cooptés», expliquera un ancien administrateur IRC d'AnonOps.

Pire encore, AntiSec en vient à hérisser certains Anons en transgressant un vieux tabou d'Anonymous: la quête de célébrité. En septembre 2011, l'un d'eux donne voix à ce point de vue en annonçant sa démission du groupe (son pseudo a été modifié):

> <ha> qu'est-il arrivé à #antisec
> <ha> laissez-moi vous raconter une histoire
> <ha> approchez-vous les enfants
> <ha> Il était une fois une équipe de hackers en quête d'un statut. La plupart d'entre eux étaient de charmantes personnes, nous avons tous nos défauts. Ils se sont fait connaître sous le nom de lulzsec.
> <ha> Ces hackers se sont dit que ce serait une bonne idée d'utiliser leur statut pour rassembler des anons contre l'industrie de la sécurité informatique.
> <ha> C'est alors que l'un d'eux a décidé de donner des mitrailleuses à des singes et de leur révéler les faiblesses des bases de données sql. Souhaitant être bien vus de lulzsec, ces singes ont hacké tout ce qui leur tombait sous la main, divulguant toute l'information qu'ils pillaient, sans égard aux conséquences et aux relations publiques.
> <ha> Les fuites de données privées ont été plus rapides qu'avec les condoms de marque WikiLeaks.
> <ha> Ils ont continué à hacker de plus belle dans l'espoir que Sabu leur donne une tape d'encouragement dans le dos.
> <ha> Puis, les vacances d'été ont pris fin.
> <ha> Ils se sont rendu compte qu'ils étaient incapables de continuer leur hacking, car des questions plus urgentes passaient

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> à l'avant-plan, comme «Avec qui vais-je m'asseoir à midi?» ou «Quel cours optionnel serait le plus sympa? Espagnol ou orchestre?»
> <ha> Ainsi prend fin la saga #antisec

Au début de l'été, les membres d'AnonOps ont tellement critiqué Barrett Brown que celui-ci a décidé de quitter le réseau. Il se targuait désormais de ne plus participer à Anonymous, et disait consacrer son énergie à Project PM, un wiki* voué à expliquer les rouages des firmes de sécurité informatique auxquelles l'État donne des contrats. Par la suite, Brown reviendra aider Anonymous dans le cadre de l'opération Cartel, une bravade dangereuse et controversée contre les cartels mexicains de la drogue. Quand ils auront enfin mis la main sur des données sensibles appartenant à la multinationale du renseignement Stratfor, les membres d'AntiSec lui transmettront de l'information pour Project PM. Mais tout cela n'arrivera pas avant quelques mois. Pour le moment, Brown est encore montré en exemple à ne pas suivre pour rappeler que la soif d'attention est mal vue.

La quête de célébrité d'AntiSec est plus difficile à cerner que celle de Brown. Contrairement à ce dernier, le groupe recherche l'attention en cultivant une image pseudo-anonyme. De plus, d'autres Anons appuient ses actions, espérant qu'elles mèneront à la divulgation de renseignements politiques classifiés ou secrets qu'il serait impossible d'obtenir de façon légale.

Mais un groupe de hackers *black hats* (sans lien avec Anonymous) en a assez d'AntiSec. Sous le nom (probablement temporaire) de BR1CKSQU4D, il publie un document dans lequel sont divulgués de prétendus renseignements personnels associés à des membres d'Anonymous et d'AntiSec. Le texte s'ouvre par une déclaration: «MERDE À ANONYMOUS! MERDE À ANTISEC! MERDE À ANONYMOUS! MERDE À ANTISEC!»

Ses auteurs ne mâchent pas leurs mots:

> Vous vous demandez pourquoi les groupes des années 1990 dont vous chantez les louanges (et dont les membres ont fondé des familles) ne

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

sortent pas de leur retraite pour venir vous aider?

Tout ce que vous avez fait, c'est user d'une rhétorique enflammée sur la «cyberguerre» et encourager l'adoption de lois en vertu desquelles des hackers seront condamnés à cinquante ans de prison.

Le plus débile, c'est que vous ne vous rendez pas compte que vous êtes la cause même de ce que vous haïssez le plus.

Chaque fois que vous menez une attaque par saturation, une firme comme Prolexic ou DOSarrest signe un contrat avec un nouveau client.

Chaque fois que vous faites une injection SQL sur un site quelconque, une entreprise de tests d'intrusion obtient un nouveau contrat.

Chaque fois que vous déclarez la cyberguerre à l'État, les sous-traitants fédéraux sont inondés de subventions.

D'autres hackers et cybercitoyens se mettent aussi à accuser Anonymous d'alimenter le complexe cyber-militaro-industriel. Notons cependant que, bien avant l'essor du collectif, des gouvernements d'un peu partout dans le monde aspiraient déjà au contrôle d'internet et adoptaient des lois peu respectueuses des droits individuels et de la vie privée. Des initiatives cybersécuritaires auraient vu le jour avec ou sans la présence d'Anonymous. Cela ne justifie pas toutes les actions du collectif, mais, devant l'ampleur des dispositifs de surveillance mis en place par l'État, il faut reconnaître qu'Anonymous a créé une plateforme flexible où les citoyens peuvent exprimer leur dissidence.

Mais BR1CKSQU4D, fidèle à sa sensibilité *black hat*, conclut sa diatribe par une série de menaces dignes de l'esprit fondateur d'AntiSec:

Si vous soutenez antisec de quelque façon que ce soit, vous serez pris pour cible.

Journalistes, musiciens, avocats, hébergeurs de sites web, fournisseurs de VPN [réseaux privés virtuels], commentateurs politiques, entreprises profiteuses... vous êtes tous des cibles valables.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Vous avez mis le pied dans NOTRE monde. Si vous ne voulez pas jouer, foutez le camp du terrain de jeu.

[...]

Nous <3 notre milieu. Merde aux médias.

BR1CKSQU4D

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Chapitre 10

Tout secret aspire à être révélé

À New York, l'été est étouffant. La canicule s'y combine à la dure réalité métropolitaine pour créer un enfer urbain dystopique. Réfléchi par les gratte-ciel de verre, le soleil est aveuglant. Des orifices s'ouvrent sur les viscères souterrains de la ville; les intestins des tunnels et les entrailles des stations de métro évacuent les citadins. Sueur, sons, scènes... Comme si cela ne suffisait pas, le New-Yorkais est assailli par des effluves putrides dignes de celles d'un durian, odeurs pestilentielles de rats morts et de déchets cuits au four par les stations de métro. Quand la fraîcheur automnale finit par arriver, la ville pousse un soupir de soulagement. Au répit olfactif s'ajoute le jaune éclatant, ambré et orangé des feuillages. Le passage à l'automne apporte un souffle nouveau: fini les sueurs nocturnes! fini la puanteur suffocante! enfin une trêve!

Le 17 septembre 2011, je me réveille à la vue d'un bouquet de délicates fleurs roses, violettes et rouges surplombant un vase enveloppé d'un masque de Guy Fawkes. C'est mon anniversaire. Le moment ne pourrait être plus opportun: aujourd'hui, à New York, on manifeste. La crise financière, la corruption, l'oligarchie et le 1 % ont marqué l'esprit de toute une génération en colère. Loin de l'atmosphère lourde, paralysante et déprimante que devrait induire l'alliance de la situation financière et de la chaleur urbaine, l'air est vivifiant. Règne un optimisme rafraîchissant qui donne envie de passer à l'action. Personne n'ose parler d'espoir (il est trop tôt pour cela), mais on sent que celui-ci pourrait naître.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Je prends mon masque et me rends au Bowling Green, près de Wall Street. En m'approchant du petit parc gazonné, j'aperçois quelques jeunes, masque de Guy Fawkes à la main. Certains me font un signe de tête, et l'un d'eux lève le pouce en me lançant: «Continuez votre bon travail!» Au début de l'après-midi, les manifestants marchent jusqu'à ce qui deviendra le centre névralgique du mouvement: le parc Zuccotti (qu'on rebaptisera Liberty Square). Les gens vont et viennent à mesure que la journée avance et qu'approche le début de la première assemblée générale, mais, en un flux incessant, de jeunes militants chargés de leur équipement de camping arrivent et s'installent.

Même si Occupy Wall Street s'est caractérisé par son enracinement en un lieu précis, on savait que les médias sociaux pouvaient et devaient y jouer un rôle essentiel. Sans être *le* – ni même *un* – déterminant majeur de la révolution, les communications en ligne ont eu en quelque sorte une fonction d'adjuvant: elles ont donné un coup de pouce essentiel au mouvement en facilitant sa coordination et en permettant aux personnes qui ne pouvaient être sur les lieux de devenir partie prenante de l'événement. Ainsi, en cette première journée d'Occupy, nous sommes nombreux à rester accrochés à nos téléphones malgré notre présence sur place. Toutes les demi-heures environ, je sors mon appareil de ma poche pour regarder mon fil Twitter. Dans l'après-midi, deux messages successifs de Sabu apparaissent. Un mois auparavant, le 16 août, Sabu s'est volatilisé après avoir publié un tweet énigmatique: «Le tour le plus formidable qu'ait joué le diable a été de convaincre le monde de son inexistence. C'est ainsi [...] qu'il a disparu[1].» Avec ces nouveaux tweets, il revient en lion: «ATTENTION: Je ne suis jamais parti, je ne suis PAS @AnonSabu ou un autre de ces poseurs. On ne m'a ni saisi, ni arrêté, ni hacké, sans parler des autres rumeurs. Toutes fausses. Trouvez-vous mieux à faire[2]!» Il poursuit avec un autre message: «Ils ont essayé de me dénoncer, de me troller, de doxer tout le monde autour de moi, de m'entraîner dans des débats interminables, mais il y a une chose dont ils sont incapables: me faire taire[3]!»

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Au début du mois d'août, Sabu m'avait prévenu qu'il entendait se faire oublier. «Le nom de Sabu finira par ne plus être nécessaire», avait-il écrit.

<biella> ah bon, ok
<biella> alors:-/
<biella> je ne dis pas qu'il l'est ni que tu devrais continuer, mais je te demande de ne pas couper les ponts, Sabu
<Sabu> eh bien
<Sabu> c'est pas comme si je m'en allais pour devenir un connard ou que je prenais la fuite
<Sabu> c'est simplement que le milieu
<Sabu> a besoin d'apprendre à trouver sa motivation en lui-même
<Sabu> pas en moi
<Sabu> j'ai l'impression que trop de gens me suivent
<Sabu> et je ne suis pas ici pour être un chef. oui je suis un chef né
<Sabu> et oui, si je le voulais, je pourrais diriger tout le mouvement, si je voulais vivre comme un dictateur
<Sabu> mais en vérité
<Sabu> je ne suis le chef de rien qui ait rapport avec anonymous
<Sabu> et, en m'en allant, j'en donne la preuve

À la suite de son départ de Twitter – et à mon insu –, Sabu a continué à fréquenter divers canaux secrets sur Internet Relay Chat (IRC). Également à mon insu (et, dans ce cas, à l'insu de ses proches collaborateurs), il a comparu au tribunal le 15 août, soit la veille de notre séance de chat. Il a plaidé coupable à l'ensemble des 12 accusations portées contre lui. Parmi celles-ci, mentionnons un chef de conspiration en vue de commettre une fraude bancaire, un chef de vol d'identité qualifié et trois chefs de conspiration en vue de mener des opérations de hacking informatique. Passible de cent-vingt-quatre ans de prison, il a accepté de collaborer avec le gouvernement en échange d'une réduction de sa peine maximale à cent ans. Il s'est aussi engagé à «ne plus commettre le moindre crime[4]».

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

En juin, à la suite de son arrestation (secrète, elle aussi), Sabu n'avait dit à personne qu'il comptait s'éclipser. En août, il a prévenu ses camarades. Les membres d'AntiSec ont l'habitude de faire des allées et venues, un facteur qui a contribué à protéger le hacker d'éventuels soupçons. Sabu a aussi établi une connexion permanente à IRC à l'aide d'un dispositif appelé «*IRC bouncer*», «proxy IRC» ou «session écran», qui lui permet de se rattacher au réseau comme bon lui semble. Il peut ainsi surveiller (avec le Federal Bureau of Investigation [FBI]) toutes les conversations en cours sur les canaux et recevoir des messages même s'il n'est pas en ligne. Ce mode de connexion ne suscite aucune méfiance, car les hackers, dont bon nombre sont accros à l'écran, utilisent souvent de tels intermédiaires techniques.

La première fois, j'avais pris ses justifications au pied de la lettre. Mais en août, il tentait également d'échapper à de graves allégations émises à son endroit juste avant sa disparition: le hacker Mike Nieves, dit Virus, l'avait accusé d'être une taupe. Les journaux de cette discussion s'étaient vite retrouvés sur Pastebin. Sabu avait commencé par insinuer qu'un membre de l'équipe de Virus était un mouchard. La réplique de Virus fut cinglante:

<Virus> quant à topiary, tu l'as balancé
<Virus> c'est tellement évident sabu
<Sabu> mon pote
<Virus> mais je ferme ma gueule
<Sabu> t'es mieux de faire attention à ta foutue gueule parce que je suis pas une taupe
<Virus> je m'en mêle pas
<Sabu> et j'ai certainement pas mouchardé mon propre camarade
<Virus> ça me dérange pas qu'«Anonymous» se fasse anéantir
<Sabu> je peux te raconter comment il s'est fait prendre
<Virus> je les ai jamais aimés, de toute façon
<Sabu> et si t'étais au courant de quelque chose, tu saurais aussi comment ça a mal fini

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<Sabu> pendant une bonne minute un troll a publié des trucs sur le twitter de topiary avec
<Virus> Anonymous n'est qu'un ramassis de loosers boutonneux obèses qui se branlent au moins 3 fois par jour dans leur sous-sol
<Sabu> «jake des shetland»
<Sabu> il avait trouvé ça sur un forum xbox
<Sabu> topiary était un gamer xbox passionné
<Sabu> connu dans le milieu, parlait beaucoup
<Sabu> un des utilisateurs du forum l'a doxé et s'est mis à balancer l'info
<Sabu> assez pour que quelqu'un avec un peu de jugeote fasse le lien
<Virus> je suis un pirate psychologique, un professionnel de la fraude d'identité, en fait
<Sabu> moi aussi, je suis un pirate psychologique[5]

Sabu tente d'abord de parer l'accusation en abreuvant Virus de compliments, en vain. Il change donc de stratégie:

<Sabu> tu sais que si je me faisais choper
<Sabu> je me livrerais
<Sabu> je suis du genre martyr
<Sabu> j'ai grandi dans la rue
<Virus> j'en ai l'intuition, et j'ai toujours raison
<Sabu> cette fois tu te trompes
<Sabu> je préfère tomber pour mes propres conneries que de faire tomber les miens

À ce moment-là, l'accusation était vraisemblable, mais certainement pas irréfutable. La prise de bec aurait tout aussi bien pu découler d'un conflit interpersonnel ou du fait que Virus fût lui-même une taupe cherchant à détourner l'attention. Ce dernier, on l'a vu, a même reconnu que ses insinuations ne reposaient sur rien de plus solide que son intuition. Fidèle à lui-même, Sabu s'est défendu de façon à la fois suave et féroce.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Quoi qu'il en soit, en adoptant un profil bas, Sabu a montré qu'il était prudent. En son absence, Anonymous s'est très bien débrouillé. Le collectif a fonctionné à plein régime pendant l'opération BART et, peu de temps après, s'est engagé dans Occupy Wall Street. Pour qu'une campagne marche bien, les Anons doivent multiplier les communications et augmenter le temps passé en ligne. Dans ces moments intenses, il n'est guère étonnant que des rumeurs se propagent à toute allure – ou s'éteignent aussi vite qu'elles apparaissent. En ressurgissant le 17 septembre, première journée d'Occupy, Sabu effectue une habile manœuvre qui renforce son aura de révolutionnaire authentique. Tel un saumon qui peut retrouver l'endroit où il est né à des milliers de kilomètres, Sabu semble programmé pour répondre présent lors de tout événement politique d'envergure. Son retour transmet le message suivant: il n'y a rien de plus exaltant qu'une campagne protestation; tout ce qui compte, c'est la révolution. Les accusations, qui semblaient justifiées par sa disparition, paraissent soudain dépourvues de fondement.

Sabu se montre très enthousiaste à l'égard d'Occupy. À mesure que le mouvement prendra de l'ampleur, il le commentera de plus en plus souvent sur Twitter. D'autres Anons partageront cet intérêt. Mais la première journée attire peu de monde. Nathan Schneider, qui deviendra un des plus éminents chroniqueurs du mouvement (sur lequel il écrira d'ailleurs un livre) dira: «Je ne croyais pas que ça pourrait durer. Je ne croyais pas que ça changerait quoi que ce soit[6].» Cependant, grâce à la persévérance des «occupants», aux médias sociaux et à la police (qui a suscité l'attention des médias et la colère du public en réprimant durement des manifestants pacifiques), les étincelles d'Occupy finiront par donner lieu à un grand feu de joie.

«Mes jours sont comptés»

Au cours de la première semaine d'Occupy, je retourne au campement à quelques reprises (et je participerai ultérieurement à quelques-unes des

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

grandes manifestations qui se tiendront à New York), mais, en tant que professeure à plein temps ayant deux cours à donner, un livre à terminer et une série de rendez-vous à honorer en vue d'un déménagement prochain à l'étranger, je peux difficilement participer au mouvement comme je l'aurais souhaité. Il arrive aussi que d'autres facteurs m'éloignent du feu de l'action. Au matin du mardi 20 septembre, ma journée s'annonce miraculeusement libre, mais la bruine qui arrose la ville m'amène à songer à tout ce que je pourrais faire d'autre de mon temps. Appelons cela le destin, mais, sans cet épisode de procrastination, je n'aurais probablement jamais rencontré Sabu en personne. Avec le recul, toutefois, je me dirai que j'aurais peut-être mieux fait de braver la pluie.

À la fin de l'après-midi, la pluie ayant cessé, je marche donc jusqu'au NYSEC, le rendez-vous informel des professionnels new-yorkais de la sécurité informatique qui se tient au bar Swift, dans Greenwich Village. J'aperçois au loin weev, le célèbre troll qui dirigeait Goatse Security et qui vit maintenant dans la région en attendant son procès. Cigarette aux lèvres, il bavarde avec deux inconnus.

weev est pompette et d'humeur joyeuse. On dirait qu'il se prépare à pousser un bon coup de gueule. Il porte un pin's de Trinity Church[7], où il assiste régulièrement à des services religieux; il prépare d'ailleurs un sermon sur Occupy. Il est difficile de savoir s'il appuie le mouvement ou s'il le perçoit simplement comme une occasion d'user de ses talents de troll. Une fois, il a prononcé un discours mémorable où il accusait les financiers véreux, condamnait la brutalité policière avec un clin d'œil à Oscar Grant et dénonçait les menaces que l'État faisait peser sur les artisans fromagers, le tout en quatre minutes. En d'autres occasions, il s'est présenté muni d'une pancarte proclamant «LES COCHONS SIONISTES NOUS VOLENT TOUS[8]». weev me salue. En entendant mon nom, un des deux hackers qui l'accompagnent hausse un sourcil: «Vous êtes la Gabriella qui fait des recherches sur Anonymous?» Je confirme. weev nous donne les dernières nouvelles d'Occupy, puis nous entrons dans le bar. Nous allons chercher à boire avant de gagner l'arrière-salle, où se trouve déjà une vingtaine de hackers. Je me dis que l'autre hacker (appelons-le Freddy) suit sans doute

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Anonymous de loin, comme le font de nombreux chercheurs en sécurité informatique. J'en viendrai cependant à constater qu'il en sait beaucoup plus que je ne l'aurais imaginé. Alors que la soirée traîne en longueur, nous nous retrouvons tous les deux dans un coin plus sombre du bar. «Êtes-vous une agente du FBI?» me demande-t-il. La question ne m'ébranle plus comme elle l'aurait fait quelques mois auparavant. Quelque peu contrariée, je lui réponds: «Non. En fait, je viens d'accepter un poste au Canada. Pourquoi le FBI m'enverrait-il dans un pays dont il fait peu de cas si je travaillais pour lui?»

Manifestement, Freddy sait beaucoup de choses sur Anonymous; il connaît par exemple l'existence des canaux secrets comme #internetfeds. J'apprendrai également qu'il a tenté d'organiser une rencontre entre Sabu et Parmy Olson, qui écrit un livre sur Anonymous. (Olson affirmerait que l'entrevue n'a pas eu lieu, même si elle admettrait avoir été en contact avec Freddy.) Au fil de notre conversation, un constat s'impose: Freddy est très proche d'Anonymous et semble connaître Sabu depuis un bon moment.

Il laisse aussi entendre que Sabu se trouve à New York, ce qui concorde avec des indices que celui-ci m'a laissés lors de nos échanges par chat. Mais Sabu fait invariablement l'objet d'un tourbillon de rumeurs, dont plusieurs veulent par exemple qu'il se soit établi au Brésil. Ce qui est tout aussi probable, car il collabore étroitement avec des hackers brésiliens et tweete souvent en portugais.

Les informations circulent dans les deux sens: je parle à Freddy de certains canaux secrets d'AntiSec et d'AnonOps, et je lui fais part de détails sur bon nombre d'opérations illégales, piquant ainsi sa curiosité. Puis, je lui apprends que j'ai grandi à Puerto Rico. En entendant cela, il offre sans détour: «Voulez-vous rencontrer Sabu?» Il pourrait organiser un rendez-vous. Complètement décontenancée, je lui réponds: «Je serais curieuse de le rencontrer, mais, honnêtement, je suis sceptique.»

Je suis emballée par la conversation, moins en raison de la perspective de rencontrer Sabu (je suis vraiment sceptique) que de l'aperçu qu'elle m'offre d'une pratique bien connue de nombreux hackers: l'utilisation du secret comme monnaie d'échange. Selon la plupart des auteurs qui se sont

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

penchés sur la question, quiconque cherche à obtenir une information peut, en livrant un des secrets qu'il possède, amener son interlocuteur à lui faire de nouvelles révélations. L'anthropologue Graham Jones, qui a étudié l'univers des illusionnistes, qualifie le partage de secrets «de marque de reconnaissance, de geste d'inclusion, de microrituel d'initiation et de participation à un système d'échange[9]». On peut partager un secret dans un esprit de vengeance ou en vue d'établir un lien de confiance. Pour faire étalage de son statut ou dans l'espoir d'obtenir une réponse. Cependant, quels que soient les motifs et les modalités du partage, la révélation d'un secret en entraîne souvent d'autres.

De retour au bar, je me pose un millier de questions. *S'agit-il d'un type ordinaire ou d'un agent de l'État? Nous nous sommes rencontrés par hasard... n'est-ce pas?* Je finis par quitter les lieux. Chez moi, épuisée, je note tous les détails dont je peux me souvenir avant de m'endormir tout habillée.

Tôt le lendemain matin, je me rends au café du coin, comme d'habitude. Deux heures plus tard, alors que je sirote ma deuxième ou troisième tasse, absorbée par mon travail, je néglige une notification venant de mon logiciel client IRC: j'ai reçu un message privé. Un délai de quarante minutes passe avant que j'active la fenêtre:

<Sabu> estas?
<Sabu> yo
<Sabu> t'es là?
<biella> salut
<biella> oui
<biella> suis là [...]
<Sabu> mira a tu foutue boîte vocale, loca [...]
<biella> lol je me demande bien pourquoi je ferais ça:-)
<biella> donner mon numéro de portable au hacker le plus tristement célèbre de tous les temps
<biella> laisse-moi d'abord écouter ma bv, mais tu connais quelqu'un qui l'a

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<biella> si je vais à mon bureau de suite est-ce que tu pourras me parler? ou je dois me contenter d'écouter ma bv?
<biella> je suis en face dans un café
<Sabu> cono biella contente-toi d'écouter puis efface

À mon bureau m'attendent un message et un numéro. J'appelle. Notre première conversation téléphonique durera une heure. Non sans arrogance, Sabu se qualifie de «hacker le plus fiable qui soit», puis demande: «C'est quoi cette foutue histoire de taupes?» Il dresse ensuite une typologie en trois volets: en premier lieu, les «infiltrés»; puis, «ceux qui veulent devenir célèbres»; enfin, «ceux qui sont au pied du mur et ne veulent pas finir en taule». Pratiquement tout ce qu'il dit contribue à me rendre aveugle à ce qu'il est lui-même. Et au cas où j'aurais des doutes, il s'acharne: «Même si le FBI avait écouté à ma porte et entendu ce que je viens de dire, il n'aurait aucune preuve d'une quelconque responsabilité technique de ma part. [...] C'est pourquoi je ne suis pas derrière les barreaux.» À ce moment-là, je trouve son explication tout à fait plausible.

Le reste de la conversation porte essentiellement sur la politique. Sabu fulmine et fanfaronne; j'écoute. Il peste contre la police de New York, qu'il juge plus corrompue que le FBI parce que portée à diffuser de fausses informations et à contrevenir à ses propres règles. Il vitupère Sony et AT&T, à ses yeux véritables criminels en raison de leur sécurité informatique déficiente. Nous abordons le cas de WikiLeaks. Selon lui, le fait qu'Assange ait raté une si formidable opportunité est une «tragédie». Il finit cependant par exprimer son admiration pour Manning.

Je parviens enfin à l'interrompre et lui demande: «Pourquoi m'as-tu contactée?»

Sa réponse est immédiate: «Mes jours sont comptés. Cette histoire doit être révélée, et les médias ne feront pas le boulot.» La conversation se termine. Je me demande ce qu'il a bien voulu dire.

Nous nous reparlerons peu de temps après. Cette fois, Sabu est dans la rue, comme l'indiquent le bruit des klaxons et les conversations qu'il tient en parallèle avec ses potes. «Les flics pourchassent un jeune Noir pour un

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

sachet d'herbe», me dit-il. Ce deuxième entretien tournera autour de sa défense du style de hacking d'Anonymous. «Nous ne sommes pas des *skids*», précise-t-il en faisant allusion à ces *skiddies* que les hackers se plaisent à tourner en dérision. Il qualifie LulzSec de «démonstration de faisabilité» dont le bilan dépasse celui de «tout autre groupe de hackers depuis quinze ans», et affirme être le concepteur d'AntiSec.

Je prends des notes à vive allure, attrapant au passage une crampe à mon pauvre poignet déshabitué de l'écriture manuelle. Somme toute, les propos de Sabu ne sont guère surprenants, du moins jusque vers la fin de la conversation. «J'espère que j'ai pas trop l'air d'un con, commence-t-il, mais je refuse de laisser mourir mes idées politiques. C'est comme ça que je me sens. J'ai l'intention de continuer à défendre l'idée d'une organisation décentralisée.» Il marque une pause avant de poursuivre: «Avec la décentralisation, c'est plus difficile de se faire infiltrer. [Mais] il y a des taupes.» Il conclut sur un ton bourru en lançant qu'il veut la «guerre». «Recursion doit être vengé pleinement. C'est un simple étudiant.» À peine quelques jours auparavant, Cody Kretsinger, 23 ans, de Phoenix en Arizona, a été arrêté par le FBI pour sa participation à l'opération menée contre Sony Pictures par LulzSec.

Lors de nos premières conversations téléphoniques, Sabu a laissé entendre qu'il aimerait que nous nous rencontrions en personne. Cette perspective m'enchante de plus en plus, mais je suis déterminée à prendre mon temps. Pour le moment, il y a beaucoup à faire, car l'engagement d'Anonymous dans le mouvement Occupy prend de l'ampleur. Des campements poussent un peu partout en Amérique du Nord et en Europe, ce qui amène une poignée de vétérans du collectif à troquer leurs jours et leurs nuits en ligne contre des jours et des nuits sur le terrain. On voit même des contingents d'occupants qui se disent Anons alors qu'ils ne se sont jamais connectés à un canal IRC de leur vie.

En une occasion, les chemins de ces deux mouvements distincts mais complémentaires se croiseront de façon saisissante. Le dimanche 25 septembre, après s'être rassemblés à Union Square, des manifestants marchent vers le sud en direction du campement jusqu'à ce que la police les

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

prenne en «souricière» et les encercle d'un genre de filet en plastique orange. Les occupants scandent «Honte à vous! Honte à vous! Qui protégez-vous? VOUS faites partie des 99 %! Vous vous attaquez à vos semblables!» Bien que personne ne l'ait provoqué, un policier haut gradé, Anthony Bologna, saisit alors sa bonbonne de gaz poivre et envoie un jet de produit vers trois jeunes femmes. Alors que le liquide leur enflamme le visage et les yeux, elles s'effondrent en hurlant: «Non! Pourquoi faites-vous ça[10]?!» Bologna, en guise de réponse, quitte nonchalamment la scène.

Des badauds ont filmé l'incident. La vidéo devient virale. Anonymous riposte sans attendre en doxant le policier, c'est-à-dire en publiant son nom et son adresse sur Pastebin avec une courte déclaration. «En observant vos policiers en train d'encercler des femmes innocentes, nous vous avons vu les asperger sauvagement de gaz poivre. Nous sommes indignés et écœurés par votre comportement. Vous savez qui sont ces innocentes; elles ont maintenant la chance de savoir qui vous êtes. Avant de commettre de nouvelles atrocités contre des innocents, pensez-y à deux fois. NOUS VOUS SURVEILLONS!!! Vous êtes prévenu[11]!»

Les données personnelles de Bologna ont été dénichées par une jeune étudiante qui, pour le mal qu'elle s'est donné, a «pris du galon» au sein de CabinCr3w. Dans l'interview qu'elle m'accorderait ultérieurement, elle m'a expliqué comment elle s'y était prise: «J'ai regardé la vidéo plusieurs fois, zoomé, tenté de mieux définir les traits du visage, le numéro de matricule, une partie du nom. Finalement, je me suis résolue à le googler, et j'ai tout simplement découvert qu'il avait fait l'objet d'une plainte.» (Un participant à une manifestation contre la convention républicaine de 2004 à New York a intenté une poursuite contre lui, laquelle est encore en suspens.)

Parce qu'elle ne m'a pas semblé être du genre à doxer par pur plaisir, je lui ai demandé où elle traçait la limite entre divulgation acceptable et violation de la vie privée: «[La police] est au service du public. Par conséquent, sa vie [...] est publique et pourrait être scrutée par un journaliste. [...] Moralement, je crois qu'il y a une limite; elle définit jusqu'où on peut doxer.» Si la jeune femme a affirmé avoir uniquement divulgué les renseignements permettant d'identifier Bologna, d'autres

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Anons ont cependant décidé d'aller plus loin en doxant les membres de la famille du policier.

Ayant d'abord défendu le geste de Bologna, le service de police de New York s'est rétracté. Une évaluation interne a établi que le policier avait enfreint le protocole. Pour le punir, on lui a retiré dix jours de vacances et on l'a réaffecté à Staten Island (ce qui en dit long sur la façon dont le service perçoit le plus petit arrondissement de la Ville)[12]. L'incident a fini par avoir aussi son bon côté: il a contribué à propulser le mouvement Occupy sur la scène nationale. *The Guardian* et d'autres grands médias ont rapporté l'événement en citant directement le message Pastebin d'Anonymous, cimentant ainsi l'association naissante entre le collectif et Occupy[13]. Occupy faisait désormais partie du décor, tant dans les milieux militants que dans les grands médias (surtout depuis l'arrestation massive de plus 700 personnes lors d'une manifestation pacifique sur le pont de Brooklyn).

À la rencontre de Sabu

En consultant une FAQ détaillée du département des technologies de l'information et des télécommunications de la Ville de New York, on peut connaître le nombre approximatif de téléphones publics qui parsèment les cinq arrondissements de la ville. «Au 2 janvier 2014, les trottoirs de la ville comptent 9 903 téléphones publics en service[14].» Je ne les avais jamais remarqués avant que Sabu ne me demande d'en utiliser un. Pour fixer la date de notre rendez-vous, il préfère éviter internet, jugeant plus prudent de recourir à un téléphone public; un ordinateur n'est jamais entièrement à l'abri d'un enregistreur de frappe.

Notre première rencontre est prévue pour le 3 octobre au Chipotle Mexican Grill de la place St. Mark, dans l'East Village. «Tu me reconnaîtras sans difficulté», m'assure-t-il. Sur le web, la seule photo qui montre prétendument Sabu est celle d'un latino sec mais musclé. J'arrive tôt. Les minutes s'écoulent, lentement. Soudain, je me rends compte qu'un

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

personnage à la stature imposante s'approche de moi d'un pas nonchalant. Déplaçant son corps massif avec aplomb, il semble être dans son élément. C'est bien Sabu. Il me serre la main si fort que je crains qu'il ne la broie. Je ramasse mes affaires, nous allons commander à manger. Alors que nous échangeons des banalités, Sabu prend une pause pour saluer la commis de cuisine, une Latina à l'air pas commode: «Quoi de neuf?»

«Ça fait un bail que je t'ai pas vu par ici», répond-elle. Qu'on se trouve au Chipotle Mexican Grill ou au parc Tompkins Square, il m'est de plus en plus clair que Sabu est connu des gens du coin, qui le traitent avec déférence. Respect ou crainte? Je l'ignore, mais nul doute qu'il est une figure importante du quartier.

Sabu a tôt fait d'orienter notre conversation vers son passé. «Je viens d'une famille de trafiquants de drogue», avoue-t-il spontanément avant de poursuivre avec nonchalance: «Quand j'avais 13 ou 14 ans, je me promenais avec 4 000 ou 5 000 dollars dans mon portefeuille.» Il m'explique également qu'il est la «figure paternelle» de ses cousines, qu'il a adoptées alors qu'elles n'avaient pas encore sept ans – pour le moment, il ne dit rien sur les raisons qui l'ont amené à prendre une si lourde responsabilité. (Quand Sabu avait 13 ans, sa tante et son père ont été incarcérés pour trafic d'héroïne. Il a été élevé par sa grand-mère jusqu'au décès de celle-ci, le 7 juin 2010, soit un an exactement avant son arrestation par le FBI. C'est à la mort de son aïeule qu'il a pris en charge les deux fillettes.)

Sabu dit avoir travaillé dur pour surmonter la «mentalité de ghetto», un cocktail de haine de soi et de colère rentrée qui paralyse. Plus tard, il me racontera brièvement quelques épisodes de sa vie où il a été confronté à un racisme des plus abjects. Sabu a été à l'école secondaire Washington Irving, située près de la 16^{e} Rue Est et fréquentée par de nombreux étudiants démunis. Un jour, il a franchi le détecteur de métal à l'entrée de l'école avec un tournevis dans sa poche. Lorsque le gardien l'a intercepté, il s'est défendu: «Je suis le geek qui répare votre système quand vous oubliez qu'il ne faut pas ouvrir les fichiers .exe "bizarres".» L'homme ne l'a pas cru, et une prise de bec s'est ensuivie. Ayant eu l'impression qu'on lui avait

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

manqué de respect, Sabu s'est plaint à la direction, mais ses récriminations sont tombées dans l'oreille d'un sourd. Il a donc décidé de faire du bruit en rédigeant une lettre virulente aux propos «controversés» (ce sont ses mots) qu'il a distribuée aux enseignants. Le directeur a qualifié la missive de «menaçante» et a infligé une suspension temporaire à son auteur. En revenant plus tard sur l'incident dans un document publié sur Pastebin, Sabu en est venu à cette conclusion: «Très bien, alors, c'est vraiment scandaleux que quelqu'un [...] comme moi soit privé d'éducation en raison de ses écrits[15].»

Les raisons pour lesquelles Sabu a trouvé dans le hacking (et ses idées élevées) une oasis pleine d'attraits sautent aux yeux. Je n'affirme pas que cet univers est exempt de préjugés, loin de là. Ce milieu, où prédominent les hommes blancs, dont certains se comportent comme des cow-boys élitistes et bravaches, est jugé aliénant et repoussant par bien des gens[16]. Les barrières sont particulièrement marquées dans les groupes underground constitués presque exclusivement d'hommes (et de quelques transgenres). Néanmoins, parce que les idées y occupent (en théorie) une place plus importante que l'origine sociale, nombreux sont les drôles d'oiseaux férus de nouvelles technologies qui y trouvent refuge[17]. Les frontières sociales érigées par les hackers ne sont pas dépourvues de contradictions: nous l'avons mentionné, si le fossé entre hommes et femmes y est immense, certaines identités (transgenres, homosexuels, handicapés) y sont courantes et bien acceptées. (Cela m'a demandé un certain temps, mais j'ai fini par me rendre compte que le salon de discussion #lounge d'AnonOps servait parfois de lieu de drague gay.) Quand Sabu indique qu'il «rencontre rarement des hackers en personne», il fait allusion au genre de liberté partielle qu'offrent, en ligne, l'anonymat et les compétences techniques.

Une fois notre rencontre terminée, je ne peux pas m'empêcher de voir en Sabu une version plus décontractée et habile d'Oscar Wao, le personnage principal de ce roman électrisant de Junot Díaz qui raconte les misères d'un nerd américain d'origine dominicaine, obèse et ostracisé, «fan de SF hardcore et de fantasy». *La brève et merveilleuse vie d'Oscar Wao* raconte l'histoire d'Oscar, qui, dans ses allées et venues entre le New Jersey et la

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

République dominicaine, avance tant bien que mal dans la vie en cherchant à vivre un rite de passage qui l'obsède: perdre son pucelage[18].

Comme Oscar, Sabu se moque des frontières. Il est à l'aise dans des environnements culturels très différents. Contrairement au personnage de Díaz, toutefois, il n'a rien d'un raté et affiche un machisme écrasant. Sur #AnonOps, il traîne une réputation de coureur de jupons; lors d'une séance de chat, il aurait écrit à la journaliste Quinn Norton: «Je vous aime bien, Quinn. La prochaine fois que vous passerez à New York, vous pourriez venir me voir hacker, nu[19].» Avec moi, il fait montre d'un peu plus de retenue, m'appelant tantôt «*mi amor*» (mon amour) tantôt «*cupcake*» (petit gâteau).

Ayant maintenant une idée plus précise du personnage, je reprends mes échanges en ligne avec lui. Le quotidien *The Guardian* lui a commandé un texte d'opinion sur Occupy qu'il me demande de commenter. De mon côté, je tente de le convaincre de se laisser filmer par Brian Knappenberger pour son documentaire intitulé *We Are Legion*:

> <Sabu> aussi
> <Sabu> si j'accepte de faire ce truc avec ton pote knapp
> <Sabu> tu dois t'assurer qu'il ne dévoile pas mon identité

Plus que tout autre journaliste couvrant Anonymous, Brian Knappenberger est entré en contact avec un vaste échantillon d'individus, investissant temps et argent dans un projet qui le passionne. Je veux l'aider. La possible collaboration de Sabu constitue une excellente nouvelle, mais je dois assurer celui-ci de ma discrétion et insister auprès de Knappenberger sur la nécessité d'une discrétion encore plus grande de sa part. J'observe généralement un protocole qui prend la forme d'«interactions en silos». Quand je chatte sur les canaux publics, un observateur pourrait se faire une idée de l'identité de mes interlocuteurs, mais, sur les canaux privés, mes échanges sont essentiellement confidentiels, ce qui respecte le protocole établi par Anonymous. Seuls deux membres de la confrérie des journalistes et des chercheurs (Knappenberger et Olson) sauront que j'ai rencontré Sabu.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Avec le recul, certaines de nos conversations en apparence futiles se révéleront beaucoup plus intéressantes. Citons par exemple l'échange suivant, survenu le lendemain de notre première rencontre:

> <Sabu> et ioerror est un chic type [ioerror est le pseudo du développeur de Tor Jacob Applebaum]
> <Sabu> j'essaie de le contacter
> <Sabu> je sais qu'il m'a soutenu l'an dernier
> <Sabu> je veux le soutenir à mon tour
> <biella> oui, il l'a fait
> <Sabu> pendant ce temps
> <biella> je le connais bien
> <Sabu> ils cherchent à lui mettre la main au collet
> <biella> depuis plus de 9 ans
> <Sabu> salue-le de ma part
> <biella> je n'y manquerai pas
> <Sabu> si nous pouvons faire quelque chose pour lui, il peut passer par toi

J'interprète alors les propos de Sabu comme un élan de solidarité. Ces conversations (et les raisons mêmes pour lesquelles il a voulu me rencontrer) finiront par prendre une tout autre signification. Le «nous» dont il est question n'est pas «Sabu et Anonymous». C'est plutôt «Sabu et le FBI» – un FBI qui bénéficie d'un accès direct à toutes les discussions du hacker, y compris celle reproduite ci-dessus. Sabu tentera à nouveau de «contacter» Applebaum par mon entremise.

Une propension à sympathiser avec autrui

En octobre, alors que le vent secoue les feuilles encore accrochées aux branches, Occupy est en plein essor. Les organisateurs diversifient leurs activités; grâce à des alliances avec les syndicats et d'autres groupes citoyens, de nouveaux flots d'indignés convergent vers Liberty Square en

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

vue d'une «journée mondiale d'action». Pendant des heures, je marche en compagnie d'une foule d'inconnus. Tout le monde semble gonflé d'énergie, bouche bée devant le dynamisme acquis par le mouvement en un mois seulement. «Les assemblées publiques d'Occupy ont apporté un grand bol d'air frais au discours politique américain», constate Nathan Schneider. «À la mi-octobre, Occupy Wall Street obtient un taux d'approbation supérieur à 50 %, soit davantage que le président Obama ou le Congrès[20].»

Défaitistes et commentateurs de tout poil accusent Occupy d'être dirigé par des bobos, de n'être qu'un feu de paille, d'être incapable de recueillir un soutien massif. Cette perception est erronée, comme en fera foi l'ampleur de la répression qui frappera le mouvement à peine un mois plus tard, lorsque de nombreux campements seront rasés aux États-Unis. Selon des documents obtenus par l'organisme Partnership for Civil Justice Fund (fondation du partenariat pour la justice civile) en vertu de la Freedom of Information Act, pratiquement toutes les instances chargées de l'application de la loi (département de la Sécurité intérieure, FBI, polices municipales, centres de fusion[21], Joint Terrorism Task Force [groupe d'intervention mixte contre le terrorisme], Naval Criminal Investigative Service [service des enquêtes criminelles de la marine] et, chose étrange, Réserve fédérale) suivent Occupy de très près[22]. Étant donné que ces documents sont largement caviardés, il est difficile d'évaluer avec précision le rôle de chacune de ces organisations. Mais on peut affirmer sans se tromper qu'elles ont «mis en œuvre un vaste dispositif de surveillance du mouvement Occupy», pour citer le titre de l'article publié sur le sujet par le *New York Times*[23]. Si Anonymous est parvenu à prospérer pendant cinq ans malgré l'arrestation de bon nombre de ses membres, c'est entre autres parce que son caractère décentralisé et son ancrage en ligne rendent son activité extrêmement difficile à anticiper. La suite des événements montrera qu'il en va tout autrement d'Occupy.

Je continue à fréquenter Sabu. Ses deux petits frères l'accompagnent parfois. Le plus âgé des deux est son acolyte. Il se montre très admiratif. Bien qu'il ne soit pas aussi expérimenté que son aîné, il adore parler informatique. Le cadet, avec ses cheveux gominés d'un noir de jais et sa

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

musculature ostentatoire, est absorbé dans ses pensées comme le sont tant d'adolescents, complètement indifférent à nos propos de geeks.

Une de nos rencontres sortira du lot. Par une soirée de novembre exceptionnellement douce, nous traînons une fois de plus au parc Tompkins Square en compagnie de ses frères avant de se rendre, seulement Sabu et moi cette fois, à l'Odessa, un *diner* new-yorkais classique au menu d'une variété hallucinante. Je peux maintenant l'affirmer avec certitude: Sabu est un animal social. En arrivant, il salue d'une poignée de main un homme que je présume être le propriétaire ou le gérant du restaurant. Nous gagnons une alcôve où nous nous laissons choir dans des fauteuils sans âge en faux cuir dont les ressorts éprouvés par le temps nous malmènent désespérément. Ce soir-là, Sabu abordera une quantité étourdissante de sujets: la gentrification, le hacker Phiber Optik, la politique au Moyen-Orient, Occupy, son chien (qui s'appelle China et souffre d'une terrible maladie de peau), la sociologie des groupes de hackers, les détracteurs d'Anonymous... et des dizaines d'autres questions qui le passionnent. De cette logorrhée, certains détails se démarquent. Pour la première fois, mon interlocuteur me parle d'un mystérieux hacker avec lequel il collabore étroitement et qu'il appelle «burn». J'apprendrai plus tard qu'il s'agit de Jeremy Hammond. Sabu adore attaquer les firmes de sécurité informatique, et il en est fier, tandis que «burn aime s'en prendre à la police». Au fil de la conversation, une chose devient de plus en plus évidente: par-dessus tout, Sabu semble se préoccuper sincèrement de ce qu'on pense non seulement de lui, mais aussi d'Anonymous dans son ensemble. Son mépris pour quiconque ose critiquer le collectif (journalistes ou internautes lambda de la twittosphère) est remarquable; il conspue toute personne qui, à ses yeux, manque de respect à son égard ou envers Anonymous. Peu après, il se détend et soupire d'un ton las: «Parfois, j'ai juste envie de tout abandonner et de ficher le camp.» Il semble effectivement exténué; depuis notre entretien précédent, il est atteint d'une toux chronique. Je sais qu'il a longuement discuté avec Olson par Skype, et je suis soudain frappée par le fait qu'il nourrit le désir ardent de voir son récit révélé à la face du monde.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Ne serait-ce que symboliquement, le port d'un masque dénote une possibilité d'hypocrisie, de duplicité, de feinte. Je suis assise en face de Sabu, je vois son visage, j'entends sa voix et je le regarde dans les yeux sans aucune méfiance, même si je sais que je ne dispose d'aucun moyen de connaître ses véritables motivations, s'il porte un masque ou non. On n'a jamais vraiment accès aux pensées d'autrui; on ne peut que tenter de jauger sa sincérité et son authenticité. Sans parler de ce que Hume considérait comme une des caractéristiques les plus durables de la nature humaine: «Nulle qualité n'est plus remarquable dans la nature humaine, à la fois en elle-même et dans ses conséquences, que notre propension à sympathiser avec les autres [...][24].»

Il est presque impossible de passer son temps à se demander quelles sont les véritables intentions des gens. Et c'est précisément cette propension de l'être humain à vouloir sympathiser qui permet au FBI d'utiliser ses taupes. Nous quittons l'Odessa. Comme d'habitude, Sabu allume une cigarette à l'odeur doucereuse. Il en prend une profonde bouffée puis confesse: «J'ai été un criminel. J'ai vendu de l'héroïne.» Et il s'éloigne.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Chapitre 11

Le sabutage

Même si AntiSec hacke sans relâche des cibles très en vue, comme le Federal Bureau of Investigation (FBI), le groupe n'attire pas beaucoup l'attention – et le peu d'attention qu'il obtient ne pourrait pas vraiment être qualifiée d'admirative. Certains Anons sont stupéfaits devant l'incohérence et le caractère aléatoire de certaines divulgations de données, dont celles qui touchent des corps policiers (Association internationale des chefs de police, association des patrouilleurs de la police de Boston, bureau du shérif du comté de Baldwin en Alabama), et les gens sont nombreux, y compris au sein d'Anonymous, à douter de leur pertinence. Défenseur des campagnes de divulgation en soi, Anonymous9 est d'avis que les opérations d'AntiSec sont vaines. «Que le menu de la cafétéria de Fort Meade soit classifié ne signifie pas qu'il soit digne d'intérêt, et encore moins qu'il vaille la peine d'être divulgué», juge-t-il. Néanmoins, juste à temps pour le «LulzXmas» (le Noël du *lulz*), un mystérieux hacker surnommé hyrriiya se présentera avec un cadeau. Le 13 décembre 2011, sur un canal Internet Relay Chat (IRC), quelques membres d'AntiSec nous prennent à part, la journaliste Quinn Norton et moi, pour nous poser une question:

> <Antisec> les journaleux vont-ils couvrir des trucs qui sont peut-être
> <Antisec> profondément illégaux
> <Antisec> lol
> <quinn> oui mais la mise en scène est importante

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<Antisec2> Pas illégaux comme les attaques par saturation ou la divulgation des courriels de policiers;)
<biella> profondément par opposition à superficiellement illégaux
<Anon> nous avons un tableau des catégories illégales
***Anon consulte l'aide-mémoire
<biella> Anon, vraiment?
<biella> lolll
***Anon se dit «merde on est baisés»
<quinn> est-ce un genre de tableau des minimums requis?
<quinn> hehe
<Anon> haha
<biella> PAS SUR LE TABLEAU illégal

Peu après cet échange, un membre d'AntiSec m'informe qu'il a en sa possession des données de cartes de crédit, et qu'il entend les utiliser pour faire des dons caritatifs. Même s'il ne me dit rien de leur origine, on est très rarement passé aussi près de me transmettre des informations à ce point sensibles. Je lui fait ma mise en garde habituelle: je ne peux pas garantir la confidentialité des renseignements qu'on me communique. Puis, le 15 décembre, comme si cela n'avait pas suffi à me faire flipper, Jeremy Hammond me contacte en utilisant le pseudo sup_g:

<sup_g> Je ne sais pas si vous souhaitez examiner des données préliminaires, si vous êtes en mesure de le faire ou s'il est prudent pour vous de le faire, mais des spools de courriels sont disponibles pour consultation.
<biella> pas maintenant, désolée:-(mais il me tarde d'en entendre parler

Mes échanges avec Hammond étaient devenus rares. La plupart de nos discussions avaient lieu dans le cadre de séances de chat collectives sur le canal privé de CabinCr3w (où il s'appelle sup_g) et sur celui du Project PM de Barrett Brown (où il s'appelle o). Avec le temps, j'avais fini par faire le lien entre ces deux pseudos, mais je demeurais perplexe quant à la véritable

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

nature du personnage. Il gardait un profil assez bas, sauf quand il était animé par des débats politiques et qu'il inondait soudain le canal de ses opinions sur un ton assez enflammé. Hammond est incontestablement le plus rebelle de la bande. Bien que son dévouement saute aux yeux, je ne pouvais m'empêcher par moments de l'imaginer en agent provocateur.

Lorsque je reçois son offre de *spools* de courriels, je suis donc troublée. Voulait-il m'inciter à commettre un délit? À ce moment-là, contrairement à Brown, dont le désir d'obtenir de tels courriels avait laissé AntiSec de marbre (il ne les avait jamais obtenus), je fais tout mon possible pour éviter de recevoir des informations de cette nature. Et, de toute façon (vu mes mises en garde répétées et la volonté des Anons de garder le silence), pourquoi m'offre-t-on subitement ces données? Ça me paraît louche et ça me stresse.

Heureusement, on me cache alors un réservoir de secrets plus profond. Le plus important d'entre eux concerne l'équipe d'AntiSec, qui, au début du mois de décembre, s'est mise à considérer Sabu avec une méfiance grandissante. Comme me l'expliquera plus tard un de ses membres, il arrivait souvent que des hackers se manifestent en affirmant avec conviction que «Sabu est une taupe». Hammond avait lui-même fini par en avoir marre des réticences de Sabu à se salir les mains, signe que quelque chose ne tournait peut-être pas rond. Mais pour le moment, chacun garde ses inquiétudes pour soi.

À la veille de Noël, AntiSec rend publics les détails de sa plus mémorable – et plus impitoyable – opération de hacking. Dans un geste de sabotage d'entreprise motivé par des impératifs politiques, l'équipe s'est infiltrée dans le réseau interne de la multinationale du renseignement Strategic Forecasting, plus connue sous le nom de Stratfor. Les membres d'AntiSec ont ainsi recueilli 50 000 numéros de carte de crédit, téléchargé cinq millions de courriels internes (couvrant une période de huit ans) et mis la main sur d'innombrables relevés. Pour couronner le tout, ils ont vidé les serveurs de tout le contenu qu'ils y ont trouvé (y compris les copies de sauvegarde). Lors de cette opération que le communiqué d'AntiSec qualifie d'«acte criminel amoureux et égalitaire[1]», ils ont tenté d'utiliser 30 000 de

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

ces cartes de crédit pour faire des dons d'un total estimé à 700 000 dollars «à la Bradley Manning Support Organization, à l'Electronic Frontier Foundation (EFF), à l'American Civil Liberties Union (ACLU), à Care International, à la Croix-Rouge américaine, à Amnesty International, à Greenpeace, à des communistes, à des prisonniers, à divers mouvements militants et à de nombreux camarades dont l'identité n'a pas été révélée[2]». (Seules 9 561 cartes étaient encore valides.) Penchons-nous maintenant de plus près sur les événements ayant mené à l'opération de hacking phare d'AntiSec.

Bordel total

Le 4 décembre, hyrriiya, qui fait partie d'une petite équipe de hackers appelée RevoluSec (qui, entre autres actions, a infiltré des ordinateurs du gouvernement syrien) contacte Sabu:

> <hyrriiya> réveille-toi
> <hyrriiya> j'ai un truc drôle que tu vas adorer
> <Sabu> je suis là
> <Sabu> quoi de neuf
> <hyrriiya>:=
> <hyrriiya> donc j'ai hacké cette firme de renseignement
> <hyrriiya> par accident

Ces propos piquent la curiosité de Sabu:

> <Sabu> on aimerait beaucoup s'introduire dans leur réseau et leurs comptes d'utilisateurs pour #antisec, transmets-moi les détails, histoire que je puisse commencer à travailler:)
> <hyrriiya>:p
> <hyrriiya> le réseau est en interruption pour le moment
> <hyrriiya> dès que j'aurai extrait ce que je cherche
> <hyrriiya> je te le donne

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> <hyrriiya> mais je vous conseillerais d'en prendre le contrôle et de les «sniffer*» pendant quelques mois
> <hyrriiya> les services secrets de mon propre pays ont recours à leurs services:p
> <hyrriiya> cnn aussi
> <hyrriiya> etc.
> <hyrriiya> the economist lol

Le lendemain, me racontera Jeremy Hammond, hyrriiya offre «à tout le canal [AntiSec] un lien vers la base de données où Stratfor compile ses commandes, laquelle comprend les adresses et les numéros de carte de crédit de sa clientèle, [ainsi que] vers d'autres numéros de carte subtilisés au hasard dans la base de données de l'entreprise». Sabu crée un nouveau canal, appelé #!sec, où hyrriiya transmet les infos relatives à l'*exploit.* Hammond me décrira le déroulement de l'opération avec maints détails techniques (non essentiels à sa compréhension):

> Pas de mot de passe! Oups! Ce qui permet d'avoir accès à toute la base de données, à partir de mysql, je peux insérer des utilisateurs dans le système drupal de str [Stratfor], créer un compte administrateur, puis valider du code PHP sur des articles drupal, insérer une porte dérobée PHP dans un article drupal permettant l'exécution de code à distance sur le serveur web de str (chaque service a sa propre boîte), puis on devient utilisateur root du serveur web et on peut se connecter à leur serveur de courriel à l'aide d'un utilisateur «autobot» qui a accès à plusieurs de leurs serveurs internes à des fins de sauvegarde, dont on devient aussi utilisateur root.

Comme si l'absence de protection par mot de passe ne suffisait pas à démontrer sa négligence, Stratfor a sauvegardé ses données de cartes de crédit en clair au lieu de les protéger par une forteresse de cryptage numérique, comme le veut la pratique courante dans l'industrie. Pour une firme qui vend des conseils en sécurité informatique, cela fait un peu un cordonnier bien mal chaussé.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

AntiSec entend balancer huit ans de courriels stockés sur les serveurs de Stratfor, ce qui représente plus de 200 gigaoctets de données. Trouver le bon endroit pour les mettre, avec suffisamment d'espace disque et de bande passante, n'a rien de simple. Hammond décide de hacker d'autres machines à cette fin. Certains membres d'AntiSec entreprennent de chercher des méthodes qui permettraient d'aller plus profondément dans les systèmes de Stratfor, tandis que d'autres, qui n'avaient pour but que de mettre le feu aux poudres, s'empressent de quitter le navire.

Le rôle d'hyrriiya se limite à celui d'intermédiaire, et il finit par se désintéresser du reste de l'opération:

<hyrriiya> et une autre chose
<hyrriiya> quand je vous aurai transmis les détails
<hyrriiya> svp oubliez qu'ils viennent de moi:)
<hyrriiya> et que revolusec a joué le moindre rôle:p
<hyrriiya> car cette entreprise est pleine de policiers fédéraux:p
<hyrriiya> et que nous n'avons pas besoin de reconnaissance.
<hyrriiya>:)
<Sabu> ouaip
<Sabu> #antisec est en guerre contre les fédéraux et l'otan depuis juin

La veille de Noël, je reçois un message d'un mystérieux utilisateur appelé ghost (un autre avatar de Hammond, apprendrai-je ultérieurement). Il me fait part de la nouvelle la plus explosive que j'aurai entendue au cours de ma recherche sur Anonymous:

<ghost> salut
<ghost> la merde est en train d'être anéantie sur anonops
<biella> salut
<ghost> m'apprête à rm -rf une cible majeure

Je ne suis pas certaine de comprendre sa première phrase, mais la seconde ne laisse aucun doute. Je ne suis peut-être pas une experte en nouvelles technologies, mais, en bonne utilisatrice de Linux depuis plus de quatorze

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

ans, je connais la signification de «rm -rf». Cette commande permet à un utilisateur root de supprimer l'ensemble du répertoire du système (dans les faits, Hammond me fait part de ses actions en abrégé, car les systèmes UNIX les plus récents sont munis de dispositifs de protection, dont le drapeau «--no-preserve-root» qu'on doit entrer au préalable, ce qui réduit le risque de suppression accidentelle après avoir tapé seulement six caractères). Je tente de garder mon calme. Je ne crois pas avoir bien compris ce dont il est question. Il me donne quelques détails:

> <ghost> c'est une importante firme de renseignement
> <ghost> dans ~30 min
> <biella> hum ok
> <ghost> en attendant, anonops se sert des cartes de crédit

J'y verrai bientôt un peu plus clair grâce à des tweets comme celui que postera Sabu: «http://www.stratfor.com #ANTISEC ANÉANTIT UNE ENTREPRISE DE RENSEIGNEMENT MULTIMILLIONNAIRE regardez la vidéo et lisez l'article. #antisec[3].» Je me dis: *Sainte Marie Mère de Dieu, c'est vraiment en train d'arriver!*

Sur les canaux publics, quelques-uns se montrent furieux, d'autres perplexes, mais la plupart semblent réagir avec humour ou juste en trolls. «LE VOTE SUR LA SÉLECTION DU BÉNÉFICIAIRE DU DON LULZXMAS SE POURSUIT; les options sont les suivantes (en ordre de préférence): CANCER, TOR, SIDA, WIKILEAKS, ABRIS, CROIX-ROUGE, ANONOPS.»

AntiSec a remplacé la page d'accueil du site de Stratfor par *L'insurrection qui vient*, un pamphlet révolutionnaire issu d'un groupe anonyme de la gauche radicale française, le Comité invisible. Ses auteurs, qui souhaitent précipiter l'effondrement du capitalisme, prônent la mise en place de nouvelles formes d'association collective et le déclenchement rapide d'«une guérilla diffuse, efficace, qui nous rend à notre ingouvernabilité, à notre indiscipline primordiales[4]». Entre Noël et le Nouvel An, les hackers redoublent d'ardeur. Souhaitant semer la pagaille, AntiSec croit nécessaire de ne pas limiter ses attaques à une seule

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

organisation. Alors que les médias se consacrent presque exclusivement à Stratfor, les hackers militants se sont en fait lancés dans une campagne de «hacking d'un océan à l'autre», ce qu'ils annoncent non sans fierté dans leur fanzine.

> À la veille du Nouvel An, alors que nos camarades révolutionnaires faisaient du bruit aux portes des prisons du monde en soutien aux incarcérés, nous ouvrions le feu sur les sites web et les courriels du 1 % en rendant publiques des informations volées aux services de police de la Californie et de l'État de New York. D'un océan à l'autre, nous avons fait triompher l'esprit du *lulz* en nous attaquant aux hauts gradés de la police: nous avons écumé leurs courriels personnels et leurs pages Facebook, malmené dans la joie leurs portails internes, subtilisé leurs documents privés, que nous nous sommes empressés de publier sur les services cachés de Tor et sur BitTorrent. Enfin, nous avons défacé leurs sites web et lancé des rm –rf sur leurs serveurs, en direct sur IRC et Twitter pour que le monde entier puisse en être témoin[5].

Les trois cibles supplémentaires d'AntiSec sont cslea.com (site de la California Statewide Law Enforcement Association, qui, il vaut la peine de le noter, se targue d'être «la plus fascinante association américaine d'organismes voués à l'application de la loi»), nychiefs.org (site de la New York State Association of Chiefs of Police) et SpecialForces.com (un marché en ligne où l'on vend de l'équipement destiné aux forces spéciales). Chacun de ces sites contribue au butin d'AntiSec, constitué de *spools* de courriels, de noms d'utilisateur, de mots de passe, de courriels, de numéros de téléphone et de documents «sensibles».

Pendant ce temps, Sabu, imperturbable, demeure implacablement culotté. À un ancien sympathisant qui reproche à AntiSec d'agir de manière irresponsable, sa réplique est cinglante: «AUX CHIOTTES la communauté du renseignement, l'industrie de la sécurité et tout ce qui se trouve entre les deux. Nous soutenons le peuple[6].» À ses yeux, les véritables criminels sont chez Stratfor: «@STRATFOR pourrait avoir contrevenu à la loi en

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

stockant les données non cryptées de ses clients sur un serveur non sécurisé, accessible au public. Posez-leur des questions[7].» De tels épisodes atténuent les soupçons dont Sabu fait l'objet chez les Anons, mais ne les font pas disparaître pour autant. Des messages à ce propos apparaissent de temps à autre sur Pastebin. L'un d'eux s'intitule «The Stratfor Hack is not the Work of Anonymous» (Le hacking de Stratfor n'est pas l'œuvre d'Anonymous) et réprimande Sabu: «Sabu et son équipe ne sont que des putes opportunistes avides d'attention et pourraient être des agents provocateurs[8].»

Quelques semaines à peine avant le LulzXmas, Sabu a enfin accepté de figurer dans le documentaire de Brian Knappenberger, mais seulement à certaines conditions. Sabu n'y apparaîtrait que caché, et sa voix devrait être modifiée. De plus, le cinéaste ne devrait laisser aucune trace numérique des déplacements nécessaires à leur rencontre. Il se rendrait à New York en payant comptant pour son billet d'avion et sa chambre (et en ayant pris soin de choisir un hôtel où l'on n'exige pas de pièce d'identité). Ayant quitté la ville pour Noël, je rentre à New York le 26 décembre sous un déluge incessant en vue d'aider Knappenberger et de faciliter son contact avec Sabu. Ce dernier ne se pointera jamais. Cependant, vu l'importance des opérations de hacking qui viennent d'avoir lieu, son absence me semble plus révélatrice de sa prudence que de l'éventualité qu'il se soit dégonflé.

Le lendemain, en dépit du lapin que Sabu nous a posé, je décide de faire un dernier effort pour le rencontrer. J'ai envie de lui offrir un modeste présent avant de quitter New York: l'essai intitulé *Les prodiges*, de Malcolm Gladwell[9]. Je descends lui téléphoner et lui demande s'il peut passer prendre le livre demain, avant que mon compagnon et moi ne partions pour le Canada. Après l'échec humide et misérable de la veille, je doute fort qu'il se présente. Mais il ne me décevra pas. Quelques minutes avant l'heure prévue pour notre départ, alors que nous prenons place dans la voiture, une grosse camionnette noire pleine de types se gare. Sabu en descend. Je sors à sa rencontre. Il est pressé, nous aussi, alors notre échange durera moins de dix minutes. Je lui donne le livre et lui souhaite bonne chance. Il s'approche de notre auto, et mon compagnon baisse la vitre. Je les présente l'un à

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

l'autre (en évitant, conformément au protocole, toute référence à Sabu ou à quelque autre nom – il ne m'a jamais donné son vrai nom). Ils se serrent la main sous l'œil de notre chien pelé. Plus jamais je ne reverrai Sabu en personne.

Revenir aux classiques

Au cours des trois mois suivants, l'activité d'Anonymous atteindra de nouveaux sommets. AntiSec a encore en main l'ensemble du *spool* de courriels de Stratfor, dont le groupe publie occasionnellement des fragments dans des communiqués de presse grinçants. De son côté, Barrett Brown persiste à réclamer les courriels, et ses relations avec le reste de l'équipe deviennent tendues. Hammond m'expliquera que certains membres d'AntiSec «n'aimaient pas BB [Brown] pour beaucoup de raisons déjà connues, liées à sa soif de célébrité». Quelques-uns d'entre eux ont été particulièrement outrés par les tweets qu'il a publiés à propos des données avant même que celles-ci ne soient divulguées.

AntiSec décide de transmettre les données à WikiLeaks. Pour ce faire, Hammond se connecte au serveur IRC de l'organisme et conclut un accord (essentiellement à l'insu de Sabu). «Les gens de WikiLeaks m'ont d'abord demandé si je pouvais authentifier la fuite en leur fournissant quelques échantillons, ce que j'ai fait, [mais] ils ne m'ont pas demandé qui j'étais ni même comment j'avais eu accès aux données; je leur ai dit de mon plein gré que je travaillais avec AntiSec et que nous avions hacké Stratfor», me racontera-t-il. Peu après, Hammond procède au transfert. En apprenant la nouvelle, Sabu exige de traiter personnellement avec Julian Assange. Après tout, explique-t-il à Hammond, il est déjà en contact avec l'assistant d'Assange, Q. (Par la suite, Kevin Poulsen publiera dans *Wired* un article sur Q, un adolescent islandais nommé Sigurdur Thordarson, dit Siggi, qui, en août 2011, a décidé de devenir taupe pour le FBI; il a ainsi transmis aux autorités des milliers de documents et de journaux de chat de WikiLeaks, «par goût pour l'aventure», aurait-il indiqué[10].) Selon Hammond, Sabu

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

entame des «discussions avec WikiLeaks dans le but d'obtenir de l'argent en échange des données», mais, à ce moment-là, le site des lanceurs d'alerte a déjà les documents en sa possession et s'apprête à les rendre publics. Deux mois plus tard, le public pourra lui-même consulter les courriels.

Vers la mi-janvier, alors que s'estompe la tempête suscitée par les dons effectués avec les cartes de crédit, le visage «proche du peuple» d'Anonymous refait surface aux États-Unis en réaction à une proposition de loi de la Chambre des représentants intitulée Stop Online Piracy Act (SOPA, loi visant à mettre un terme au piratage en ligne). Ce projet d'une portée considérable suscite une vive opposition, et pas seulement chez les libertariens. Le milieu de l'informatique et l'élite de Silicon Valley le condamnent également. S'il était adopté, le SOPA contraindrait entre autres Google et les autres moteurs de recherche à empêcher certains sites, tel The Pirate Bay, d'apparaître dans leurs résultats. Le projet de loi a suscité le lancement d'une vaste campagne de protestation qui culmine le 18 janvier 2012 par une action web d'une ampleur sans précédent: la «journée de black-out». Une poignée de grandes sociétés internet, de nombreux groupes de défense de l'intérêt public et des milliers d'individus ornent leurs sites de logos noirs et de liens permettant aux visiteurs d'écrire à leurs représentants pour exprimer leur opposition au SOPA. Environ 75 000 sites web d'entreprises privées et d'associations à but non lucratif sont mis hors ligne, et non les moindres: Wikipedia, Flickr, *Wired*, 4chan et Google font partie du lot[11]. La presse publie des tonnes d'articles sur le sujet. CBS News qualifie le nombre de participants à la campagne de «stupéfiant»: 4,5 millions de personnes ont signé la pétition que Google a fait circuler; 350 000 citoyens ont écrit à leurs représentants par l'entremise de SopaStrike.com et d'AmericanCensorship.org; plus de 2,4 millions de tweets portant sur le SOPA ont été publiés au cours de la seule journée du 18 janvier; une pétition mise en ligne sur le site de la Maison-Blanche a recueilli 103 785 signatures[12]. Après une semaine de campagne, le gouvernement annonce officiellement l'ajournement, pour une période indéfinie, du SOPA et de son pendant du Sénat, la proposition Preventing Real Online Threats to Economic Creativity and Theft of Intellectual

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Property Act (PIPA, loi sur la prévention des menaces en ligne réelles à la créativité économique et du vol de propriété intellectuelle): «Nous entendons maintenir notre collaboration avec les deux partis représentés au Congrès en vue d'élaborer une législation qui offrira les nouveaux outils nécessaires au combat mondial contre le piratage et la contrefaçon, tout en défendant avec acharnement un internet ouvert, fondé sur les valeurs que sont la liberté d'expression, le respect de la vie privée, la sécurité et l'innovation[13].»

Des sociétés géantes comme Google, des personnalités respectées d'internet comme le cofondateur de Wikipedia Jimmy Wales et des organisations de défense des libertés civiles comme l'EFF ont toutes contribué à la victoire. Mais le contingent des geeks et des hackers de la base (qui comprend bien sûr Anonymous) a aussi joué un rôle déterminant. En plus de produire des vidéos et des affiches pour la campagne, il a publié de constantes mises à jour sur plusieurs comptes Twitter très suivis. Une fois le black-out terminé, par contre, les acteurs du secteur privé se sont dépêchés de sortir des feux de la rampe. Anonymous et ses semblables, eux, ont poursuivi la lutte – qui paraissait sans fin.

Dès le lendemain, en effet, soit le 19 janvier 2012, les autorités fédérales américaines font fermer le populaire site de partage de fichiers Megaupload. Le grégaire et controversé fondateur de l'entreprise, Kim Dotcom, est arrêté en Nouvelle-Zélande lors d'un raid matinal spectaculaire. Pour les militants d'Anonymous, la disparition de ce site ne présage rien de bon. Bien que l'arrestation de Dotcom n'ait strictement rien à voir avec le SOPA, elle témoigne encore une fois de l'immense pouvoir des industries détentrices de droits d'auteur sur le contenu web, avec ou sans loi pour les soutenir: même si, pour le moment, aucun tribunal n'a reconnu Dotcom coupable de piratage, on a saisi sa propriété et fait disparaître son site web. (Au moment où j'écris ces lignes, l'affaire de Dotcom est toujours pendante, mais le premier ministre néo-zélandais John Key a présenté des excuses officielles à l'homme d'affaires pour la surveillance illégale ayant mené au raid, auquel ont participé 76 policiers soutenus par 2 hélicoptères[14].)

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Anonymous réplique à la fermeture et à l'arrestation en lançant la plus vaste campagne d'attaques par saturation de son histoire. Le collectif bloque les pages d'accueil de Universal Music, du FBI, de l'office du droit d'auteur des États-Unis, de la Recording Industry Association of America (RIAA), de la Motion Picture Association of America (MPAA) et d'autres organisations qui, comme celles-ci, tentent d'éradiquer le partage de fichiers. Anonymous et AnonOps ont cependant changé de tactique en optant pour un autre logiciel que Low Orbit Ion Cannon (LOIC). Appelé PyLoris, le nouvel outil est à la fois mieux conçu et plus puissant; aspect plus important encore, il protège l'identité de ses utilisateurs. Il fonctionne en établissant avec le serveur visé une connexion incomplète qui reste active pendant une très longue période. Normalement, un serveur dispose d'un nombre limité de «prises» (*slot*) destinées aux connexions. En cas de connexion partielle, la «prise» attend, refusant toute nouvelle requête. Si des internautes établissent et maintiennent un nombre suffisant de connexions incomplètes, les «prises» du serveur sont toutes occupées et le service est interrompu.

Tout se déroule à la façon des meilleures opérations de la vieille école: le logiciel est téléchargeable à partir d'un lien publié sur un canal IRC, et les cibles sont annoncées sur le canal aux quelques milliers de personnes qui ont décidé de participer à l'attaque. Des liens mènent aussi vers des guides permettant d'apprendre comment rendre sa connexion anonyme à l'aide de Tor et d'un réseau privé virtuel (VPN).

À peine quelques semaines plus tard, l'Europe est le théâtre d'importantes manifestations en ligne et dans les rues contre l'Accord commercial anticontrefaçon (ACTA), un autre projet de traité international sur le droit d'auteur. Anonymous est encore de la partie. En réaction à la décision du gouvernement polonais de ratifier l'ACTA, le collectif bloque plusieurs de ses sites web et promeut énergiquement les manifestations prévues à Cracovie. Peu après, lors d'une audience parlementaire sur l'ACTA, les députés du mouvement Palikot, un parti politique progressiste de Pologne, décident de porter des masques de Guy Fawkes. C'est une première: jamais des élus n'ont adopté le symbole révolutionnaire

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

auparavant (et aucun ne le refera par la suite). En juillet 2012, devant le tollé de protestations, le Parlement européen rejette le projet d'accord.

Par la suite, un Anon de la première heure, qui était membre de #command à une époque aussi lointaine que l'automne 2010, me contacte:

<h> ces temps-ci, on dirait qu'il y a un nouveau groupe
<h> sans lien avec #antisec [et] qui travaille plus que jamais
<h> ce qui me rend heureux et fier
<biella> ouais
<biella> ici et ailleurs
<biella> c'est bien
<h> et quand j'ai vu ces politiciens polonais
<h> avec leurs masques
<biella> ouais, surréaliste
<h> j'ai réalisé que la bande de fous que nous sommes est entrée dans la conscience collective
<h> et qu'elle change les choses à petite échelle
<h>:D

Qu'un Anon s'enorgueillisse du succès d'Anonymous est tout naturel. Mais il y a autre chose: le constat qu'il fait de l'influence croissante du collectif semble juste. Peu de temps après cet échange, en effet, j'ai reçu un appel d'un investisseur en capital-risque qui avait participé à l'organisation de manifestations contre le SOPA. Il voulait en savoir plus sur la façon dont Anonymous s'organisait dans l'ombre. Le collectif semblait toujours surgir de manière imprévisible, constatait-il, avant de me demander si je croyais possible que quelqu'un de l'extérieur entre en contact avec Anonymous et réoriente son activité vers d'autres enjeux que la liberté du net. Je trouvais son idée plutôt grossière (un des principes d'Anonymous veut que le collectif ne devienne jamais l'armée personnelle de qui que ce soit), mais l'intérêt qu'éprouvait ce financier démontre tout de même la justesse de l'intuition de h: Anonymous était désormais un ingrédient actif du cocktail politique mondial.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

«N'admettez rien, niez tout et lancez des contre-accusations»

Le 27 février 2012, WikiLeaks rend disponibles les courriels de Stratfor sous le titre «The Global Intelligence Files» (dossiers du renseignement mondial). Les opinions divergent quant à leur portée politique. Une poignée de journalistes, d'experts en sécurité informatique et même de clients de la firme réagissent par un simple «bof». Les preuves d'agissements répréhensibles ou illégaux sont minces, affirment-ils. Cette réaction blasée est influencée par la réputation alors peu enviable de Stratfor, dont nombre d'observateurs considèrent qu'il s'agit d'un repaire d'escrocs: «Stratfor est une blague, et il en va de même pour WikiLeaks, qui la prend au sérieux», lance un Max Fisher cinglant dans le magazine *The Atlantic*[15]. Moyennant un tarif exorbitant (40 000 dollars par an en 2001), les abonnés de Stratfor reçoivent un bulletin d'information qui, selon Fisher, ne contient guère plus que du réchauffé. Et, sans surprise, la réputation de la firme en prend encore pour son grade lorsqu'on apprend qu'elle n'a jamais fait l'effort de crypter les données des cartes de crédit de ses clients.

Cependant, d'autres journalistes et citoyens sont plutôt d'avis que les courriels ont une portée politique bien réelle en ce qu'ils fournissent des éléments de preuve des pratiques moralement douteuses de Stratfor, telles la propagande d'entreprise déguisée en relations publiques ou la surveillance de militants. Les courriels de la firme sont effectivement très révélateurs – et parfois même prémonitoires, comme en fait foi cet extrait d'un long courriel tapé, chose remarquable, sur un iPhone, le 10 décembre 2010:

> Les channeurs/anon/b sont instruits et sont à la fine pointe de la technologie des réseaux. Ils forment une nébuleuse, présente un peu partout dans le monde, constituée de gens loyaux, dépourvus de tout sentiment nationaliste et unis par leur intérêt commun pour le chaos (le *hentai* et les chats, bon sang). Ils sont souvent parvenus à révéler l'identité et les renseignements personnels d'un individu à partir d'une seule photo (d'une femme jetant un chat à la poubelle, par exemple),

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> et ils ont dispensé une justice digne de milices à des gens avec qui ils sont en désaccord. [...]
>
> Il sera très intéressant de surveiller ce que les Anons vont faire dans l'environnement «post-WikiLeaks». Si cette bande de geeks vivant au sous-sol chez maman se transforme en mouvement digne de ce nom, ils pourraient causer de sérieux ennuis et s'avérer difficiles à éliminer. [...] les quelques déséquilibrés qui se trouvent parmi eux pourraient avoir un impact destructeur s'ils le voulaient[16].

Le journaliste Steve Horn passera au peigne fin des milliers de courriels de Stratfor et publiera un dossier en deux volets sur les tactiques de la firme et des entreprises de la fusion desquelles elle est issue, soit Mongoven, Biscoe and Duchin (MBD) et Pagan. Le fondateur de MBD, Ronald Duchin (un militaire doté d'une longue expérience en relations publiques), a lancé la «formule Duchin», qui consiste «à isoler les radicaux et à "cultiver" les idéalistes en vue de les "éduquer" à devenir réalistes, puis à récupérer les idéalistes en les amenant à partager les vues de l'industrie». Horn constatera que cette stratégie «est encore en vigueur chez Stratfor»[17].

La majorité des courriels divulgués témoignent du fait que «Stratfor se démarque par son service d'analyse sociologique destiné à renforcer le pouvoir des milieux d'affaires et le capital, et non par un vil travail de terrain», explique Horn[18]. Un petit nombre de messages font état d'une surveillance plus directe des militants. L'explosion de 1984 à l'usine d'Union Carbide de Bhopal, en Inde, une des pires catastrophes industrielles du XX^{e} siècle, a fait des milliers de morts et a exposé plus de 500 000 personnes à des produits chimiques hautement toxiques. Dow Chemical, qui a acheté Union Carbide en 1999, a fait appel à Stratfor pour garder l'œil sur divers groupes militants, dont les Yes Men et le Bhopal Medical Appeal, qui faisaient connaître l'enjeu ou fournissaient de l'aide aux victimes. Les documents divulgués révèlent aussi que Coca-Cola a embauché Stratfor pour surveiller l'association People for the Ethical Treatment of Animals (PETA, association de défense des animaux), en particulier ses opérations canadiennes à l'approche des Jeux olympiques

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

d'hiver de 2010 à Vancouver. La firme a aussi dépêché un employé, qui se qualifiait lui-même d'«agent secret», au sein du groupe local d'Occupy à Austin, au Texas, en vue de recueillir des renseignements, c'est-à-dire de suivre le moindre mouvement des occupants et d'explorer leurs liens potentiels avec des militants écologistes:

> Il y a un groupe, que vous connaissez peut-être, qui s'appelle Deep Green Resistance. [...] J'ignore si la police fédérale ou qui que ce soit d'autre le considère comme écoterroriste, mais c'est bien ce qu'il est, et il devrait être surveillé. [...] Les membres de sa section locale d'Austin étaient parmi la foule devant l'hôtel de ville, mais les choses n'étaient pas assez «radicales» à leur goût, car travailler au sein du système n'a pour eux aucune pertinence. Le 5 novembre, alors que j'étais infiltré, certains de mes contacts m'ont dit que, pendant l'assemblée générale du 4, des conflits ont éclaté entre des membres ordinaires d'Occupy et Deep Green[19].

Ces exemples nous ramènent aux enjeux soulevés dans le chapitre 7 relativement aux courriels de HBGary et de HBGary Federal, lesquels contenaient, entre autres propositions tout aussi effrayantes qu'invasives, celle de discréditer WikiLeaks. Bien que l'espionnage au service des entreprises reste un phénomène mal connu, ces révélations de pratiques peu scrupuleuses, couplées à la difficulté d'avoir accès aux documents des sociétés privées, nous empêchent de rester indifférent devant les liens étroits entre l'industrie et le gouvernement. Si, comme le prétend un des courriels, le vice-président au renseignement de Stratfor, Fred Burton, applique bel et bien la maxime «N'admettez rien, niez tout et lancez des contre-accusations», on voit alors toute l'importance des fuites et du rôle de lanceur d'alerte joué par Anonymous et ses semblables.

Stratfor publie une déclaration à propos de l'authenticité des courriels divulgués: «Certains courriels pourraient avoir été falsifiés ou modifiés et contiendraient ainsi des inexactitudes; d'autres pourraient être authentiques. Nous ne nous prononcerons pas sur leur véracité. Nous ne nous prononcerons pas non plus sur leurs idées sous-jacentes. On nous a volé ce

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

qui nous appartient, et nous ne jouerons pas les victimes une seconde fois en nous soumettant à un interrogatoire à ce propos[20].»

Stratfor commente cependant deux courriels qui, par la suite, seront largement reconnus comme faux: une lettre de démission du fondateur, directeur des technologies de l'information et PDG de la firme, George Friedman, écrite par AntiSec, et un courriel contrefait que Stratfor aurait envoyé à tous ses clients pour leur offrir, en guise d'excuses pour la fuite, un abonnement gratuit à son bulletin d'information.

«J'avais besoin que la vérité sorte»

Cet hiver-là, Sabu se montre plus arrogant et provocateur que jamais en public. Début février, en réponse à un détracteur qui l'interroge sur une rumeur voulant qu'AntiSec ait en sa possession des courriels syriens, Sabu rétorque: «Vous allez tous ravaler vos paroles quand nous aurons décidé de balancer ce que nous avons. Les gouvernements, nous n'en avons rien à foutre. Seul le peuple nous intéresse[21].» Nous ne nous sommes pas parlé depuis mon départ pour le Canada. Cette interruption n'est pas attribuable aux seuls aléas du déménagement: à Montréal, quiconque utilise un téléphone public en plein hiver court des risques d'engelure. Mais, tôt dans la matinée du 6 mars, Sabu me harcèle sur Twitter. Il veut que je l'appelle dans les plus brefs délais, peu importe la manière. Je prends donc le téléphone de mon appartement et compose son numéro.

Sabu me donne l'impression d'avoir commencé à parler avant de répondre: «Fox s'apprête à diffuser une info à propos de moi et du FBI.» Il m'indique que l'information doit être publiée dans quelques minutes à peine, et qu'il souhaite m'expliquer certaines choses avant que j'en prenne connaissance. Désemparé, il estime que les gens de Fox «ont commis la pire bassesse» en s'en prenant à lui et à sa famille, mais il refuse de me dire ce qu'ils ont fait exactement. «Ce n'est pas ce que tu penses», se contente-t-il de préciser. J'ai la tête qui tourne. Je suis en colère. Je peine à verbaliser

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

ce que je ressens. Je retiens mal ce que Sabu est en train de me dire. Puis, je ne sais trop comment, la conversation prend fin.

Finalement, ce n'est pas un mais trois articles sur Hector Xavier Monsegur qui sont publiés sur le site de Fox, chacun accompagné d'un gros plan de son visage capté devant son écran d'ordinateur. On a découvert le pot aux roses: Sabu collabore avec le FBI. C'est ce qu'il a essayé de me dire au téléphone. Je suis estomaquée. La nouvelle coïncide avec une série d'inculpations dont les articles donnent aussi les détails. Aux États-Unis, le FBI vient d'arrêter Jeremy Hammond. Au Royaume-Uni et en Irlande, Ryan Ackroyd (Kayla), Donncha O'Cearbhaill (Palladium) et Darren Martyn (pwnsauce) sont accusés de conspiration par ordinateur.

La nouvelle se répand sur les différents canaux IRC telle une onde de choc. Sur le canal #CabinCr3w sont présents des gens très proches de Sabu (les pseudos ont été modifiés):

<round-eyes> camarade, page d'accueil de Foxnews
<round-eyes> tout de suite
<kama> ok
<round-eyes> la vache
<flava-flav> meeerde
<flava-flav> je savais pas
<flava-flav> aïe
<flava-flav> enculé de sabu
<flava-flav> les mecs
<flava-flav> je peux parler?
<flava-flav> une minute
<Nacho-King> vas-y
<Mega> NON
<Mega> lol blague vas y
<comrade> lol
<flava-flav> on doit voir ça comme un moment décisif
<Nacho-King> ^
<flava-flav> comme en libye après khadafi

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<flava-flav> nous voilà libérés d'un fardeau
<flava-flav> d'une tare
<flava-flav> qui entachait tout ce que nous étions
<flava-flav> et allions devenir
<Mega> mais il n'avait rien d'un fardeau au début, selon moi
<comrade> ouais, ce qui se passe est pas rassurant flava-flav
<flava-flav> et à partir de maintenant
<Mega> pourquoi pas comrade
<flava-flav> vous comprenez pas ce que je veux dire
<flava-flav> il représente une phase
<flava-flav> et maintenant
<comrade> lol
<flava-flav> nous entrons dans une phase nouvelle
<comrade> ok
<comrade> une phase, ça me va
<comrade>:D
<flava-flav> c'est un processus évolutif
<Nacho-King> ok flava-flav je dis juste que beaucoup de gens réagissent, et de plein de façons

Nacho-King voit juste. Bien que tout le monde se sente trahi, une minorité d'Anons persiste à défendre Sabu. L'article de Fox News rapporte d'ailleurs que le FBI a posé au hacker un bon vieil ultimatum qui a fait ses preuves: soit il collaborait avec la police fédérale, soit on lui retirait la garde de ses cousines. Certains membres d'Anonymous (plus parasites que hackers chevronnés) me raconteront par la suite que, à l'été 2011, Sabu les a invités à «foutre le camp». Manifestement, ce dernier s'est rapproché des Anons possédant les habiletés requises pour s'introduire dans un système, et ne s'est pas occupé de ceux qui ne contrevenaient pas à la loi. Il a visé les éléments qui présentaient un plus grand intérêt pour le FBI.

Au bout de quelques heures, un sentiment commence à prédominer sur les canaux, lequel fait écho aux propos d'un porte-parole du gouvernement

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

non identifié, cité dans le reportage de Fox: «Dans le milieu du hacking, on peut devenir un messie, mais on reste toujours une ordure.»

À la fin de la journée, la réputation de Sabu au sein d'Anonymous est ternie à jamais. En se propageant sur internet, la nouvelle suscite des hurlements de rage et un douloureux sentiment de trahison. Ce n'est qu'au bout d'un mois que ma propre colère se sera suffisamment apaisée pour que je puisse avoir une nouvelle discussion avec Sabu.

Plus teigneux que jamais, il amorce le dialogue en déplorant amèrement que «personne n'ait émis le moindre doute sur le reportage», puis grommelle qu'il n'en revient pas d'être traité comme un «déchet toxique».

«J'ai protégé des centaines de personnes», affirme-t-il avec force. «J'en ai sauvé, des culs. Quand tu as des enfants, tu dois faire un choix. J'ai fait ce qu'il fallait faire.» Son seul appel à la sympathie se rapporte aux sanctions judiciaires qu'il encourt. Après tout, il s'est fait arrêter et est en liberté sous caution; il risque toujours une peine de dix à quinze ans de prison. Il trouve «stressant» de ne pas savoir ce qui va lui arriver. Quand je lui demande jusqu'à quel point il a fait et dit ce que le FBI attendait de lui, il s'emporte: «Tout ce que j'ai dit sur Twitter venait de moi!» Plus tard, il ajoutera: «J'étais sincère dans mes tweets, personne ne m'a dicté quoi écrire.» Cette affirmation contredit les propos de l'agent traitant de Sabu rapportés par Jana Winter de Fox News: «Environ 90 % de ce qu'on lit en ligne, c'est des salades», a-t-il affirmé à propos des messages de Sabu sur Twitter et des «interviews» qu'il a accordées à la presse[22]. Que l'agent dise vrai ou qu'on soit en présence d'une campagne de désinformation élaborée et insistante, il apparaît que le hacker a bêtement répété ce que le FBI lui demandait de dire. On sait aujourd'hui que, dans certains tweets («Si Dieu rendait mon arrestation impossible, j'assumerais la responsabilité de mes crimes et me livrerais aux autorités. Je crois injuste de faire tomber les autres pour mes propres péchés. Merci[23].»), Sabu racontait de pures salades, préparées sous l'influence du FBI. J'arrive difficilement à placer un mot, mais je parviens tout de même à lui demander s'il est venu à ma rencontre sous ordre du FBI. Il proteste d'une voix encore plus forte: «Nom

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

de Dieu! Pas besoin d'une permission pour aller manger un *burrito* au foutu Chipotle!» Insatisfaite de sa réponse, je lui demande encore pourquoi il est entré en contact avec moi à la base, et lui pose une question supplémentaire sur le type qui a rendu notre rencontre possible (le hacker du NYSEC). Il commence par tourner autour du pot, puis s'interrompt d'un coup. «J'avais besoin que la vérité sorte d'une manière ou d'une autre», déclare-t-il avec lucidité. «Plus nous passions de temps ensemble, plus j'avais l'impression que je pourrais me confier à toi. Une situation merdique.»

Il se laisse ensuite aller à un déluge de propos acrimonieux: «Je m'attendais à ce que les nerds exposent ma famille, pas les médias. Parce que les médias ont publié de la merde sur ma famille! Il ajoute: Il y a beaucoup d'informateurs au sein d'Anonymous.» Il conclut par quelques élans de reconnaissance, dont un éloge de «Jeremy et Doncha», deux hackers parmi les plus calés et les plus travailleurs d'Anonymous qui se sont toujours refusés à toute collaboration avec les forces de l'ordre (et dont l'arrestation est largement attribuable à Sabu). Enfin, il m'offre ces mots d'adieu: «Je crois toujours qu'Anonymous est une idée magnifique. La décentralisation, c'est le pouvoir.»

Des mouchards qui contreviennent à la loi

À peu près au même moment, des membres d'Anonymous et certains journalistes indépendants, dont Nigel Parry, remettent en question le discours des autorités sur le hacking de Stratfor. Le 25 mars 2012, Parry publie un billet de blog étoffé, intitulé «Sacrificing Stratfor: How the FBI Waited Three Weeks to Close the Stable Door[24]» (Le sacrifice de Stratfor: pourquoi le FBI a attendu trois semaines avant d'agir). Selon lui, il est très étrange que la firme ait pu se faire hacker systématiquement sous les yeux de la police fédérale. Le FBI soutient (tant dans les documents qu'il a remis à la Cour que dans le reportage de Fox) que Monsegur est resté sous haute surveillance pendant toute la durée de sa collaboration. «Selon les autorités,

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

les activités en ligne de Sabu étaient épiées 24 heures sur 24 par un agent du FBI», écrit Jana Winter[25].

Grâce à Monsegur, le FBI pouvait suivre directement, en temps réel, le déroulement des opérations, ce qui lui a permis d'informer Stratfor de l'intrusion presque immédiatement, début décembre. AntiSec n'avait alors accès qu'à la base de données sur la clientèle. Hammond n'infiltrerait pas le reste du système avant dix jours, et n'effacerait pas les données avant dix autres jours, à la veille de Noël. Stratfor avait donc amplement le temps d'améliorer la sécurité de son système ou à tout le moins de faire une copie de sauvegarde de ses données. Mais la compagnie ne l'a pas fait. Dans la foulée de la campagne de hacking, son PDG, George Friedman, ne fournirait que de vagues explications à ce propos: «Nous travaillions à améliorer notre infrastructure de sécurité dans les limites du temps dont nous disposions, et dans celles qu'imposait notre volonté de protéger l'enquête: nous devions empêcher les attaquants de savoir que nous étions au courant de leur intrusion[26].»

En novembre 2013, des dossiers judiciaires rendus publics confirmeront la chronologie des événements présentée par Hammond. Pourtant, pendant plus de deux ans, aucun journaliste ne se sera donné la peine de questionner Stratfor sur les raisons pour lesquelles l'entreprise n'a pas pris de mesures de protection supplémentaires à la suite de la première intrusion. De plus, personne n'aura cherché à savoir pourquoi le FBI a attendu jusqu'au 24 décembre pour transmettre une deuxième fournée de mauvaises nouvelles à Stratfor (le téléchargement des courriels et la suppression des données), alors qu'il savait pertinemment qu'AntiSec disposait depuis quelques jours d'un meilleur accès au système de la firme.

La justification fournie par le FBI ne permet guère d'y voir plus clair. «Le FBI a déclaré qu'il avait informé Stratfor sans attendre, mais a précisé que, à ce moment-là, il était déjà trop tard», écrit Nicole Perlroth dans le *New York Times*. «Dans les semaines qui ont suivi, des hackers ont fouillé dans les données financières de Stratfor, dans ses courriels et dans les renseignements personnels et financiers de ses abonnés, en supprimant à

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

l'occasion des données parmi les plus précieuses, le tout au vu et au su des agents du FBI[27].»

En mai 2014, les journalistes Dell Cameron et Daniel Stuckey mettront la main sur une masse impressionnante de documents judiciaires ayant fait l'objet d'une fuite (journaux de chat, photos de surveillance, documents produits par le gouvernement lors du procès de Hammond). Ceux-ci leur permettront de corroborer la chronologie de Hammond avec une plus grande précision. Les journaux de chat, en particulier, contribueront à la confirmation d'«accusations de longue date en vertu desquelles les enquêteurs fédéraux, dans le cadre de leur traque de Hammond et d'autres membres d'Anonymous, ont permis à un informateur de contrevenir de façon répétée aux lois relatives à la criminalité informatique», écrira Cameron[28].

Les allégations voulant que Sabu ait apporté un soutien logistique et moral à la perpétration d'actes illégaux (rappelons que c'est lui qui a informé Hammond de la vulnérabilité de Stratfor) ne se limitent pas à l'opération contre Stratfor. Au cours de l'audience de détermination de sa peine, Hammond lit une déclaration qui contient une autre accusation explosive:

> Après Stratfor, j'ai continué à m'introduire dans d'autres cibles en utilisant un puissant «*exploit* jour zéro» qui me donnait le statut d'administrateur dans des systèmes munis de la populaire plateforme d'hébergement web Plesk. À maintes reprises, Sabu m'a demandé un accès à cet *exploit*, et j'ai refusé. Ne disposant pas de son propre accès, il a continué à me fournir des listes de cibles vulnérables. J'ai infiltré bon nombre des sites web dont il m'avait communiqué les coordonnées, téléchargé les comptes de courriel et les bases de données sur le serveur du FBI utilisé par Sabu, et transmis à ce dernier (et, par le fait même, au FBI) les mots de passe et les portes dérobées qui permettaient de prendre le contrôle des cibles. Ces intrusions, qui m'ont toutes été proposées par Sabu alors qu'il collaborait avec le FBI, ont touché des milliers de noms de domaine appartenant en

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> grande partie à des gouvernements étrangers, dont ceux du Brésil, de la Turquie et de la Syrie[29].

Alors que Hammond s'apprête à mentionner d'autres cibles étatiques, le juge Preska lui demande: «M. Hammond, nous venons de parler de la nécessité de taire le nom de ces pays. J'aimerais que vous n'en fassiez pas mention.» Dans sa déclaration, Hammond rappelle aussi au tribunal l'existence de preuves soutenant ses affirmations:

> Tout cela s'est déroulé sous le contrôle et la supervision du FBI, ce qui peut être confirmé facilement par les journaux de chat que nous ont remis les autorités conformément à leur obligation de communication des pièces dans le cadre de ce procès. [...] Parce que j'ai plaidé coupable, je n'ai pas eu accès à de nombreux documents qui auraient pu m'être remis avant le procès, dont les communications de Sabu avec le FBI. De plus, la majorité des documents qu'on m'a fournis font l'objet d'une «ordonnance de protection» qui empêche le public de les examiner.

La déclaration de Hammond est reproduite en ligne. Certains sites caviardent les noms des pays mentionnés, d'autres non. Ayant été informée de ces opérations de hacking la première fois que j'ai rendu visite à Hammond en prison, en septembre 2013, j'en suis venue à me demander jusqu'à quel point ses affirmations étaient vraies. Après avoir fait part de mes interrogations à des journalistes, j'ai fini par convaincre Mark Mazetti de mener une enquête, qui déboucherait, fin avril 2014, sur un article à la une du *New York Times*: «FBI Informant is Tied to Cyberattacks Abroad» (Taupe du FBI impliquée dans des cyberattaques à l'étranger)[30]. Une fois divulguée la masse de documents judiciaires sous ordonnance de protection, les journalistes Daniel Stuckey et Andrew Blake ont publié un compte rendu détaillé du rôle joué par Sabu dans l'orchestration des opérations contre les sites web du gouvernement brésilien et de diverses entreprises. Bien que Sabu ait confié bon nombre de ses cibles aux bons soins de Hammond, il a aussi fait part de vulnérabilités à d'autres hackers. Dans un

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

cas attesté, il a offert un précieux *exploit* qui «permettait d'ouvrir les portes dérobées de centaines de sites web brésiliens[31]». Le tout sous le regard bienveillant du FBI.

Le fait que le FBI ait autorisé Sabu à faciliter une vaste campagne de hacking illégal (ou ait à tout le moins toléré qu'il le fasse) est perçu comme un odieux abus de pouvoir par beaucoup d'Anons. Bien entendu, on ne sait pas (et on ne saura probablement jamais) si les services de Sabu ont été prêtés par le FBI à d'autres agences (au sigle de trois lettres) aux fins d'opérations militaires ou de collecte de renseignements, si ses actes ont indirectement servi les objectifs du gouvernement lui-même, et si d'autres facteurs ont joué un rôle. Mais, en situant l'affaire dans le contexte plus large du système américain de recours à des informateurs, on constate vite qu'un tel scénario n'a rien d'inhabituel. La professeure de droit Alexandra Natapoff soutient que les relations douteuses entre informateurs et agents traitants ne relèvent pas de l'exception: elles sont même très répandues. Dans un essai intitulé *Snitching: Criminal Informants and the Erosion of American Justice* (Le mouchardage. Les informateurs criminels et l'érosion de la justice aux États-Unis), elle expose de façon convaincante un système tordu qui a souvent pour effet d'encourager la criminalité et la violence. Selon Natapoff, le FBI autorise systématiquement ses taupes à contrevenir à la loi tant que celles-ci se montrent coopératives. Bien que le mouchardage soit un outil indispensable du système judiciaire, conclut-elle, dans le cadre des programmes actuels, «le recours aux informateurs est très dommageable pour l'intégrité du processus de justice criminelle[32]».

Natapoff et des journalistes ont documenté de nombreux cas d'abus de pouvoir. En 2005, par exemple, un élève ingénieur à mi-temps établi en Californie a été escorté hors de l'avion qui devait l'emmener de Paris à San Francisco. Même s'il était détenteur d'une carte verte et ne faisait pas l'objet d'une enquête, on l'a interrogé pendant des heures dans une salle du service américain des douanes et de la protection des frontières. Finalement, un agent du FBI l'a placé devant une alternative: soit il devenait informateur au sein de la communauté musulmane des États-Unis, soit on le déportait vers son pays d'origine, le Maroc[33]. En avril 2014, quatre

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

hommes musulmans ont intenté une poursuite judiciaire contre Washington: ils soutenaient que le FBI les avait inscrits et maintenus sur une liste d'interdiction de vol après qu'ils eurent refusé d'espionner des communautés musulmanes des États de New York, du New Jersey et du Nebraska[34]. En se livrant à cette forme d'intimidation, les autorités interviennent directement sur un milieu, transforment sa nature, alors qu'aucun acte répréhensible n'y a été officiellement constaté.

Aux États-Unis, la majorité des affaires impliquant des informateurs n'aboutissent pas devant les tribunaux, si bien qu'une bonne partie de ce qu'on sait du système – et l'essentiel des arguments brandis pour réclamer sa réforme – est attribuable à de rares procès et aux fuites (on voit ici en quoi la divulgation de documents issus du procès de Hammond a pu servir la démocratie). Le fait qu'on ait autorisé Sabu à contribuer à tant d'opérations de hacking au vu et au su du FBI démontre que le système de recours à des informateurs est entaché d'irrégularités persistantes, et rappelle douloureusement que l'État n'hésite pas à employer des méthodes à la fois légales et illégales pour démanteler un mouvement qu'il juge menaçant.

«Ne faites confiance à personne sur IRC, jamais»

Alors que se propage la nouvelle sur le statut d'informateur de Sabu, on réalise que, même si la collaboration de ce dernier avec les autorités a eu un impact déterminant, de nombreux participants aux opérations ont négligé de protéger adéquatement leurs renseignements personnels. Anonymous9 résume cette prise de conscience ainsi: «Si des gens se sont fait arrêter à cause de lui, c'est en partie parce qu'il était un traître, et en partie parce qu'ils ne faisaient pas attention. S'ils n'avaient pas partagé des renseignements personnels avec lui, ils n'auraient pas été inquiétés. Ça nous ramène en quelque sorte à ce dicton: "Ne faites confiance à personne sur IRC, sous aucun prétexte."»

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Il peut être difficile de prouver qu'un crime informatique a été commis, à moins de trouver des données accablantes sur l'ordinateur du suspect (numéros de carte de crédit, courriels, etc.). Toutefois, comme l'explique le chercheur en sécurité informatique Robert Graham, les journaux de chat fournis par une taupe peuvent servir à «faire condamner une personne pour conspiration, intention de nuire à autrui, entrave à la justice [et] racket[35]». Et, dans le cas qui nous occupe, la poursuite n'a pas manqué de journaux de chat pour soutenir sa cause. Reste que la présence de Sabu n'a pas suffi pour mettre le grappin sur tout le monde: certains membres d'AntiSec et de LulzSec courent toujours. Si les autres avaient mieux pris soin de leur sécurité opérationnelle, ils ne se seraient peut-être pas fait attraper.

Comment ces erreurs ont-elles été commises? Hammond appliquait des règles de sécurité opérationnelle presque sans faille, mais, lors de séances de chat, il a révélé certains détails de sa vie personnelle. Sa confidence la plus déterminante (dont j'ai été témoin une fois sur un canal public et une autre fois sur un canal privé) a été celle de la peine qu'il avait purgée dans une prison fédérale. Avec un de ses principaux pseudos, Anarchaos, le fait, assez particulier, qu'il ait été un des rares hackers anarchistes authentiques à avoir été écroué dans une prison américaine a dû lui assurer une position assez élevée dans la liste des suspects potentiels. Une des tâches les plus indispensables qu'ait accomplies Sabu a sans doute été de faire des liens dans le florilège de pseudos de Hammond. Voici un court extrait, tiré des documents judiciaires, d'une conversation entre Sabu («CW-1») et Hammond («@sup_g») tenue le 25 décembre:

<CW-1> quelles sont les nouvelles?
<@sup_g> j'ai travaillé toute la nuit
<CW-1> il paraît que tous les journaux parlent de nous
<CW-1> à cause de vous, bande d'enfoirés, la police va débarquer chez moi
<CW-1> HAHAHAHA

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

<@sup_g> nous publions 30 000 cartes, les données de it.stratfor.com et une autre déclaration
<@sup_g> mec c'est gros
<CW-1> s'ils débarquent chez moi, anarchaos, tu devras semer le chaos en mon honneur
<CW-1> <3
<CW-1> sup_g:
<@sup_g> je vais le faire

Évidemment, Sabu s'est avéré essentiel aux enquêtes de bien d'autres façons. Un jour, un membre de LulzSec a partagé avec lui un lien vers une vidéo «maison» qu'il avait postée sur YouTube. Munies de l'URL, les autorités ont fait parvenir à YouTube une assignation à produire l'adresse associée au compte; dès lors, il leur a été facile de trouver la page Facebook de l'Anon. Ce jeune hacker avait commis la grave erreur d'y publier des captures d'écran incriminantes du défaçage d'un site web, qui ont ensuite été partagées avec un autre membre de LulzSec (oy vey).

Ne faire confiance à personne sur IRC, comme le prône Anonymous9, n'est pas si simple. Si le «sabutage» (ainsi a-t-on nommé l'affaire avec humour) a fait si mal, c'est parce qu'Anonymous, à l'instar de la plupart des mouvements politiques, repose entre autres sur des amitiés, voire sur des relations plus intimes. Des séances de chat sur le canal privé de l'équipe ont donné lieu à des mariages, comme celui qui a uni le jeune hacker John Anthony Borell III (Kahuna) de CabinCr3w à son épouse Sarah. Topiary a pris soin d'un de ses amis de LulzSec qui traversait une période difficile. Même des Anons n'ayant jamais échangé leurs coordonnées entretiennent des liens solides et durables. Par conséquent, un tel contexte procure un sentiment de bien-être qui peut amener à se trahir en parlant trop. Pour qui reconnaît l'existence du problème, changer de pseudo en prenant soin d'effacer toute trace de son identité précédente et en adoptant un ton différent ne va pas de soi. Selon Parmy Olson, les hackers sont constamment acculés à ce «dilemme»: changer de pseudo implique de

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

renoncer à un marqueur d'identité stable et à une réputation essentielle à toute collaboration à long terme entre hackers[36].

J'ai demandé à quelques Anons pourquoi Sabu, étant donné les soupçons qui planaient régulièrement sur lui, était non seulement toléré, mais a pu devenir la figure publique d'AntiSec. Pour O'Cearbhaill, membre d'AntiSec, c'est grâce à son charisme. Comme nul autre, Sabu savait enflammer les passions avec ses appels au soulèvement. De nombreux Anons avancent une autre explication plausible: un autre personnage flamboyant, Yettie (pseudo modifié), faisait lui-même régulièrement l'objet d'accusations de mouchardage, ce qui détournait l'attention de Sabu. Au moins dix membres actifs d'Anonymous m'ont fait part de leurs craintes à l'égard de Yettie. Actif sur d'innombrables serveurs IRC, ce hacker avait une réputation de manipulateur (j'ai moi-même eu l'impression d'y goûter). À l'automne 2011, au cours de la brève période où il agissait sous le pseudo de crediblethreat, Hammond lui a d'ailleurs fait passer un mauvais quart d'heure lors d'un conflit interne exceptionnellement étalé en public:

> <crediblethreat> hé yettie
> <crediblethreat> as-tu expliqué à tout le monde
> <crediblethreat> comment et pourquoi on t'a chassé de la bande restreinte d'antisec?
> <crediblethreat> où étais-tu pendant ces longs mois? [...]
> <crediblethreat> pourquoi diable te ferait-on encore confiance, mouchard?

À ce jour, personne n'a encore déterminé avec certitude si Yettie était un informateur ou simplement un sombre personnage. Beaucoup d'autres Anons ont fait l'objet d'insinuations. Les rumeurs du genre sont toujours évaluées à l'aune de ce que l'on considère comme un comportement bizarre et des rares informations factuelles dont on dispose. Dans les documents policiers qui ont été divulgués, par exemple, il était question d'un «CW-2» (*cooperating witness 2*, témoin coopérateur 2), ce qui laissait entendre qu'au moins deux taupes s'affairaient dans les parages (selon certains documents, elles auraient été au moins cinq)[37]. De nombreux Anons se

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

sont aussi demandé pourquoi certains hackers et participants intégrés aux canaux secrets n'avaient été ni arrêtés ni interrogés une fois sortis de l'ombre. Un tel climat d'incertitude favorise l'atmosphère de paranoïa orageuse et ambiguë dont tant de mouvements de gauche ont été imprégnés. Une fois la peur et la confusion installées, il devient «difficile de distinguer la paranoïa de la réalité, les ennemis imaginaires de ceux qui sont bien réels», explique Ruth Rosen, auteure d'un essai sur la peur induite par le FBI au sein du mouvement de libération des femmes dans les années 1960[38].

La révélation du rôle de Sabu a aussi mis Anonymous à l'épreuve en poussant le collectif à entrer dans une période d'introspection. Pendant des semaines, alors qu'ils gémissaient, fulminaient, faisaient le point, refaisaient le point et piquaient des crises sur Twitter et divers réseaux IRC, les Anons se sont demandé quel pourrait être l'avenir d'Anonymous (si avenir il pouvait y avoir) après un tel coup dur. Pour reprendre les propos d'un haut gradé de la police cité dans l'article de Winter sur Fox News, «s'ils apprenaient que leur dieu collabore avec l'État, les hackers seraient complètement terrorisés».

Toc-toc-toc! C'est nous!

Le sabutage a certes attisé les flammes de la paranoïa, mais il n'est pas venu à bout d'Anonymous – ni n'a vraiment suscité la terreur dans ses rangs. Même si le collectif n'a jamais retrouvé l'effectif qu'il avait à l'époque de LulzSec et d'AntiSec (et qui avait valu aux Anons le surnom de «hackers dopés aux stéroïdes»), il s'est plutôt bien débrouillé tout au long de l'année 2012 et pendant une bonne partie de 2013, en menant des opérations un peu partout dans le monde. Rien ne pourrait mieux illustrer sa redoutable réputation que l'anecdote qui suit, issue des plus hauts échelons de l'appareil d'État américain.

En 2012, l'équipe de la campagne pour la réélection de Barack Obama décida de réunir un groupe de programmeurs, d'administrateurs de système,

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

de mathématiciens et de spécialistes des données pour mieux identifier les électeurs potentiels. Admirative de ces technologues chevronnés et indépendants d'esprit, la presse fit état de leur travail acharné, en soulignant leurs réussites et les difficultés rencontrées – elle finirait d'ailleurs par encenser le système dont ils accoucheraient. Les articles omirent cependant de rapporter une des principales préoccupations du groupe. Tout au long de la campagne, en effet, les technologues ont considéré Anonymous comme une source d'ennuis potentiellement plus importante que ne l'étaient les hackers qui, pour le compte de puissances étrangères, avaient infiltré les campagnes d'Obama et de McCain en 2008[39].

À la fin novembre, le journaliste et geek militant Asher Wolf constata que Harper Reed, technologue en chef de l'équipe électorale d'Obama, était abonné à @AnonyOps sur Twitter. Faisant un *trickster* de lui-même, il communiqua l'information à AnonyOps: «Amusons-nous avec ça, et voyons ce que ça va donner», suggéra-t-il[40].

AnonyOps envoya donc à Reed un message privé: «Salut. Les mois qui viennent s'annoncent chauds. Peut-être devrions-nous chatter.» Reed lut le message. «Mon cœur s'est arrêté de battre», m'a-t-il confié plus tard. Il contacta aussitôt son patron, le directeur des technologies de l'information et le chef de la sécurité de la campagne d'Obama. Après avoir ébauché diverses réponses en 140 caractères, Reed et ses trois collègues eurent un éclair de génie: «Salut. Qu'as-tu en tête?» Au moment où le technologue s'apprêtait à envoyer le message, le directeur des technologies de l'information, qui venait d'en discuter avec les avocats chevronnés qui collaboraient à la campagne, se précipita pour interrompre son geste. Il avait changé d'avis: la meilleure réponse, finalement, consistait à ne pas répondre du tout. Mais il arriva quelques secondes trop tard.

Si Reed avait su ce que je savais, il se serait évité un jour ou deux de stress. AnonyOps voulait simplement engager une discussion avec un personnage politique influent. Lors d'une interview qu'il m'accorderait, Wolf reviendrait sur l'événement:

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> Nous nous sommes bien amusés, nous étions comme des enfants qui défient les limites [...] de la superpuissance mondiale. Nous étions passés à travers l'année 2010, alors que la rage déferlait sur les écrans parce que le gouvernement s'en était pris à WikiLeaks, et nous étions passés à travers Occupy [...]. Nous avions vu des gens incarcérés, disparaître. [...] Peut-être étions-nous devenus un peu fatalistes. Et peut-être nous disions-nous que, pour une fois seulement, il serait agréable de s'approcher de cette administration qui bombarde de petits enfants avec ses drones pour lui écraser une cigarette au visage.

Cet incident montre qu'Anonymous est devenu un véritable spectre. L'influence du collectif est désormais si grande qu'il n'a plus besoin de faire quoi que ce soit pour avoir un effet. Il est tout à fait compréhensible que l'équipe électorale d'Obama ait été troublée par ces coups ambigus frappés à sa porte numérique. Dans les deux mois qui ont suivi l'arrestation de Hammond, Anonymous a hacké des centaines de sites web de l'État chinois, mis le site de Formula One Administration hors ligne après que le gouvernement répressif du Bahreïn (où devait avoir lieu le prochain Grand Prix de Formule 1) eut emprisonné des protestataires, et hacké le site du ministère des Finances de la Grèce afin d'attirer l'attention sur un projet de surveillance des comptes bancaires des citoyens qui participait de la lutte contre la fraude fiscale. Au printemps 2012, les Anons ont lancé une autre opération d'envergure contre le site de la Formule 1, laquelle coïncidait cette fois avec le Grand Prix de Montréal; ils souhaitaient ainsi dénoncer la «loi 78», une mesure controversée du gouvernement du Québec qui visait à étouffer la contestation née de sa volonté d'augmenter les droits de scolarité universitaires. La Commission des droits de la personne et des droits de la jeunesse du Québec a publié une analyse de 56 pages où elle condamnait la loi, qui contrevenait de manière flagrante à la Charte québécoise des droits et libertés de la personne en raison notamment d'un article en vertu duquel le fait d'organiser une manifestation de 50 personnes ou plus en omettant de transmettre l'itinéraire aux autorités au moins huit heures à l'avance était passible d'une amende de plusieurs milliers de dollars[41]. Ce même

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

printemps, en Inde, après qu'un arrêt de la Cour suprême eut ordonné aux fournisseurs d'accès internet du pays de bloquer les sites d'échange de torrents, les sites de partage de fichiers et même certains sites de partage de vidéos, Anonymous a riposté en lançant des attaques par saturation contre la Cour suprême, le ministère des Communications et des Technologies de l'information, le département des Télécommunications, le parti Bharatiya Janata et le parti du Congrès national indien. Comme bien des Anons, les membres d'AnonOpsIndia ont utilisé Twitter pour faire entendre leur point de vue: «Nous continuerons à #EMMERDER le gouvernement jusqu'à ce qu'il cesse de #censurer notre #INTERNET. IL NOUS APPARTIENT[42]!»

En 2013, Anonymous a poursuivi ses activités de plus belle. Le collectif a continué de s'attaquer à des enjeux persistants, notamment dans le cadre de l'opération Last Resort (dernier recours), une campagne de hacking vengeresse contre le département de la Justice des États-Unis et la commission américaine de détermination des peines lancée dans la foulée du suicide du militant et pionnier d'internet Aaron Swartz. La famille et les admirateurs de Swartz considèrent que son suicide à l'âge de 26 ans est un geste politique motivé par le désespoir qu'il éprouvait en attendant son procès. Il risquait trente-cinq ans de prison et un million de dollars d'amende pour avoir téléchargé des articles scientifiques qu'il n'avait pourtant jamais partagés. «La mort d'Aaron [...] est le produit d'un système de justice où règne l'intimidation et où les procureurs vont trop loin», ont écrit sa conjointe et sa famille[43]. Dans la vidéo produite pour ses défaçages, Anonymous reprend cette affirmation: «Il y a deux semaines aujourd'hui, une limite a été franchie. Il y a deux semaines aujourd'hui, Aaron Swartz est mort. Mort parce qu'il faisait face à un dilemme insoluble. Mort parce qu'on l'avait forcé à jouer une partie qu'il ne pouvait pas gagner – une perversion abjecte de la justice –, une partie qu'on ne peut gagner qu'en refusant d'y jouer[44].»

Par la suite, trois opérations nord-américaines portant sur une série d'allégations d'agressions sexuelles et de viols, d'abord traitées avec indifférence par les médias, se mirent à susciter l'intérêt des fabricants de nouvelles. Anonymous se retrouva alors sous les feux de la rampe. À

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

nouveau dans sa position favorite, le collectif parvint à stimuler le débat public sur un enjeu souvent traité comme un triste spectacle.

La première affaire, qui avait eu lieu à Steubenville, en Ohio, concernait deux membres d'une équipe de football américain accusés d'avoir violé une camarade de classe. Pendant la nuit de l'agression, des coéquipiers avaient photographié et filmé la femme évanouie, puis s'étaient empressés de partager les images sur les médias sociaux, force commentaires nauséabonds à l'appui. Une vidéo, sur laquelle Anonymous allait bientôt la main, montre un étudiant affirmant fièrement: «Ils l'ont violée plus durement que le flic qui viole Marsellus Wallace dans *Pulp Fiction.* [...] C'est comme ça qu'on sait qu'elle est morte, parce que quelqu'un lui a pissé dessus[45].»

Michelle McKee, une militante de Steubenville, était convaincue qu'un procès impartial était impossible dans une ville qui traite ses joueurs de football comme des demi-dieux. En décembre 2012, elle décida donc de faire appel à Anonymous, qui fondit sur sa proie en moins de temps qu'il ne faut pour le dire. Un Anon, qui avait adopté depuis peu le pseudo de KYAnonymous (Deric Lostutter, de son vrai nom) et qui était alors absorbé par la mission qu'il s'était donnée (celle de dévoiler l'identité des participants aux forums de porno rancunière [*revenge porn*]), cet Anon, donc, ne manqua pas de faire connaître sa fureur sur Twitter lorsqu'il apprit le viol de Steubenville. McKee décida alors de lui envoyer les fichiers incriminants qui avaient circulé sur les comptes de réseaux sociaux des individus impliqués dans l'affaire. KYAnonymous sauta dans l'arène. Il commença par diffuser un avertissement vidéo hautement menaçant, que David Kushner décrirait de façon mémorable dans le magazine *Rolling Stone*: «Tel un habile joueur de poker, Lostutter émaille son manifeste d'un bluff. Il prétend qu'Anonymous a déjà doxé "tous ceux impliqués" dans le crime et dans la tentative d'étouffer l'affaire (parents, enseignants, enfants), et que le collectif s'apprête à mettre en ligne leurs coordonnées, "à moins que, d'ici le Nouvel An, tous les accusés se manifestent en publiant des excuses publiques à la jeune femme et à sa famille[46]".»

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Le lendemain, le hacker Noah McHugh, qui agit sous le pseudo de BatCat, affirma s'être infiltré dans RollRedRoll.com, le portail web des équipes sportives de l'école (dont le nom s'inspire de leur mascotte, un étalon rouge et musclé aux traits diaboliques), et dans son *spool* de courriels. Pendant ce temps, KYAnonymous tweetait sans relâche, et des vedettes comme Roseanne Barr faisaient connaître la cause à un public plus large. Le 29 décembre, par une froide journée d'hiver, un millier de manifestants répondirent à l'appel d'Anonymous et envahirent les rues de Steubenville, arborant comme il se doit leurs masques de Guy Fawkes. «L'événement a pris une tournure dramatique quand certaines participantes ont enlevé leurs masques et ont parlé à la foule des agressions sexuelles et des viols qu'elles avaient elles-mêmes subis», écrirait Kushner.

L'affaire continuerait à occuper Anonymous sur Twitter jusqu'à ce que deux adolescents soient reconnus coupables de viol en mars 2013. L'un d'eux reçut la sentence minimale d'un an dans un établissement correctionnel pour jeunes, tandis que l'autre écopa de deux ans. En novembre 2013, le *New York Times* annonça que quatre citoyens de Steubenville, dont l'administrateur régional des écoles, étaient accusés d'avoir dissimulé les preuves d'un viol antérieur[47]. En juin 2013, le FBI fit une descente chez Lostutter, qui faisait face à une inculpation en vertu de la Computer Fraud and Abuse Act (CFAA); Noah McHugh aurait quant à lui été arrêté en février. S'ils sont reconnus coupables, les deux hommes encourent des sentences plus lourdes que celles des violeurs.

Autre affaire. En avril 2013, Anonymous eut vent du triste sort de Rehtaeh Parsons, une excellente étudiante ayant mis fin à ses jours après avoir été victime d'intimidation. Les pressions auraient suivi une agression sexuelle dont elle aurait été victime lors d'une fête arrosée à Halifax, en Nouvelle-Écosse. Si aucun des jeunes hommes incriminés n'avait été accusé, affirmait Anonymous, c'est parce que la Gendarmerie royale du Canada (GRC) n'avait pas traité l'incident comme elle l'aurait dû. Des Anons s'employèrent donc à faire connaître l'affaire en publiant une vidéo et un communiqué de presse intimant la GRC de faire le nécessaire pour que les suspects soient traduits en justice sans délai. Leah Parsons, la mère

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

de Rehtaeh, fit toutefois savoir qu'elle préférait que justice soit rendue par les autorités, et non par des justiciers du net. Les participants à l'opération Justice for Rehtaeh respectèrent ce souhait en publiant une déclaration sans équivoque:

> Contrairement à ce que véhiculent les médias, nous nous opposons à ce que la justice soit affaire de justiciers. Adhérer à cette idée reviendrait à applaudir le passage à tabac de ces violeurs par une foule déchaînée. Ce que nous voulons, c'est que justice soit rendue. Et c'est votre boulot. Alors faites-le. Nous tairons les noms des violeurs jusqu'au moment où nous considérerons avec certitude que vous n'avez pas l'intention de rétablir la justice pour la famille de Rehtaeh. Sachez que d'autres groupes d'Anons souhaitent aussi divulguer ces informations, et qu'ils n'ont peut-être pas l'intention d'attendre plus longtemps. Nous vous conseillons donc d'agir au plus vite[48].

La GRC a fini par rouvrir l'enquête, mais a minimisé le rôle d'Anonymous en affirmant que les nouvelles preuves «ne provenaient pas d'une source en ligne[49]». Les Anons et certains commentateurs ont au contraire considéré que les activistes masqués avaient fait toute la différence: «Il ne fait aucun doute que la pression émanant d'internet a joué un rôle décisif dans cette affaire», a observé Emily Bazelon, de *Slate*[50]. D'abord ambivalente, Leah Parsons en est venue à être reconnaissante envers Anonymous. Fin août 2013, la GRC accusa les deux hommes de production et de distribution de pornographie juvénile (en novembre 2014, le premier reçut une absolution sous conditions après avoir plaidé coupable; en janvier 2015, le second fut condamné à douze mois de probation, également après avoir plaidé coupable[51]).

La troisième opération d'Anonymous a porté sur une affaire qui ne s'était jamais rendue devant les tribunaux, parce que le procureur avait jugé la preuve insuffisante. Les faits sont les suivants: après une fête à Maryville, dans le Missouri, Matthew Barnett, 17 ans, déposa Daisy Coleman, 14 ans, devant chez elle, par un temps glacial; à peine consciente, l'adolescente, qui ne portait qu'un t-shirt et un pantalon de jogging, faillit mourir de froid.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Deux enquêtes approfondies de la presse locale avaient clairement laissé entendre que la preuve contre Barnett était plus que suffisante pour que des accusations soient portées contre lui. Dans un article où elles comparaient la situation aux événements de Steubenville, Peggy Lowe et Monica Sandreckzi, de Kansas City Public Media, citaient ainsi le shérif de Maryville: «Est-ce qu'un crime a été commis? Certainement. Est-ce que c'était un crime horrible? Oui, c'en était un. Et est-ce que ces garçons devraient être punis pour l'avoir commis? Absolument[52].» Aussitôt ces articles portés à son attention, Anonymous se mit à faire beaucoup de bruit, amenant ainsi le pays entier à s'intéresser à l'affaire. Finalement, un procureur spécial déposa officiellement un chef d'accusation contre Matthew Barnett: méfait de mise en danger d'un enfant.

Les interventions d'Anonymous dans ces trois affaires ont provoqué de vives réactions et n'ont pas fait l'unanimité. Journalistes, féministes et simples citoyens ne se sont pas entendus sur la question de savoir si les opérations du collectif avaient aidé les victimes ou leur avaient porté préjudice. Dans un article cinglant paru dans le magazine *The New Yorker*, Ariel Levy tomba à bras raccourcis sur Anonymous (et les autres cybermilitants) en affirmant que tout l'attrait du collectif reposait sur l'adhésion naïve du grand public à un archétype simpliste, celui d'un groupe «de Peter Parker contemporains, des nerds de l'informatique qui revêtent un costume pour se transformer en super-héros justiciers[53]». D'autres observateurs ont été plus nuancés et sont allés au-delà de l'argument du justicier. Dans une interview vidéo diffusée sur *Huffington Post Live*, l'auteure féministe Jaclyn Friedman a livré ses réflexions sur l'«arme à double tranchant» que constituait selon elle le cybermilitantisme: «La personne agressée est victime une première fois, puis le redevient lorsque les photos et les vidéos se mettent à circuler. Néanmoins, dans certains cas, comme on l'a vu à Steubenville, où Anonymous a fait connaître les vidéos, de tels documents peuvent devenir des preuves, augmentant ainsi les probabilités que justice soit rendue[54].»

Quoi qu'il en soit, aux États-Unis comme au Canada, Anonymous a suscité un débat public cruellement nécessaire sur la culture du viol. Dans

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

un article captivant du *New York Times Magazine*, Bazelon décèle un fil conducteur entre ces trois «opérations de chevaliers blancs», lequel fil remonte également à un échantillon plus large des actions politiques du collectif, et ce, même lorsque ces dernières n'ont aucun lien avec la fonction de justicier. Quand Anonymous se jette dans la mêlée, c'est généralement parce que ses membres perçoivent ce qu'ils considèrent comme une injustice. Et, dans bon nombre de cas, les faits finissent par leur donner raison[55]. Interviewée, en complément à son article, au sujet de ses recherches sur le collectif, Bazelon ajoute: «Selon moi, chaque opération doit être jugée séparément. Tout bien considéré, celles auxquelles participent des gens vraiment responsables sont sans doute bénéfiques. Je crois que c'est le cas de Maryville et peut-être aussi de l'affaire Rehtaeh Parsons, bien que celle-ci soit plus controversée parce qu'un innocent a été accusé. Quant aux autres, elles ont dérapé.»

En effet, l'opération de Steubenville – celle qui a le plus attiré l'attention des médias – a été à maints égards la moins bien menée des trois. Entre autres accrocs, la victime s'est elle-même fait doxer, et des citoyens de la ville ont subi du harcèlement. En publiant la vidéo, Lostutter a indigné de nombreux Anons (et, une fois le document en circulation, la colère n'a fait que s'intensifier, car l'homme affichait une tendance flagrante à l'autopromotion).

Deux réserves méritent aussi une réflexion plus approfondie. Premièrement, si les justiciers posent problème en ceci qu'ils contournent le processus judiciaire, ils se manifestent parce que l'accès à la justice est déficient, voire inexistant. Trop souvent, on montre les «justiciers» du doigt tout en ignorant ou en minimisant les conditions systémiques qui rendent leur existence possible. En second lieu, les équipes sont capables de s'ajuster. J'ai été témoin d'une telle dynamique à dix reprises au moins. Après les erreurs de Steubenville, les interventions d'Anonymous dans des affaires de viol ont été menées avec plus de délicatesse, un meilleur suivi et une plus grande bienveillance. Bien sûr, une telle capacité d'adaptation est fragile: les groupes de travail du collectif sont prompts à se dissoudre. Ils fonctionnent bien pendant trois ou six mois, puis implosent dans un fracas

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

de querelles internes. (Bazelon relate en détail les débats orageux ayant mené au démantèlement de l'un d'eux.) Il arrive qu'ils se reconstituent au bout d'un certain temps avec de nouveaux membres qui n'ont pas assimilé les leçons apprises à la dure par les autres.

Contrairement à d'autres regroupements de hackers et de geeks (telle Debian, la plus grande organisation vouée au logiciel libre du monde), Anonymous ne dispose pas de méthode établie pour s'instituer. Seuls des protocoles limités – et provisoires – sont consacrés à la prise de décision, à la reproduction sociale et au mentorat. Le canal IRC #opnewblood, par exemple, remplit des fonctions essentiellement pédagogiques. Il s'agit d'un lieu où les nouveaux venus peuvent se familiariser avec la culture et les technologies d'Anonymous. Certains comptes Twitter, tel @YourAnonNews (qui a déjà compté 25 collaborateurs tenus de respecter un guide de rédaction), sont de véritables mini-institutions médiatiques (@YourAnonNews a d'ailleurs déjà été taxé de micro-impérialiste).

En dressant le bilan de la constellation des pratiques d'Anonymous, on peut tirer quelques grandes généralités. Les Anons ont tendance à se passer de codes réglementaires stricts, auxquels ils préfèrent des réactions ad hoc, ponctuelles, adaptées aux événements. Ils sont même en lutte contre la mémoire institutionnelle, y compris lorsque des Anons ou des médias immortalisent une opération. Pour sûr, le collectif fait preuve d'une grande cohésion culturelle, assurée par ses innombrables vidéos, mèmes et autres coutumes. Mais, en même temps, Anonymous évite ou refuse d'implanter des politiques et des méthodes transposables de gestion de ses opérations. Mais cette tendance ne se résume pas à la seule allergie des Anons à la formalisation: vu le caractère unique de chaque opération, il pourrait s'avérer très difficile d'implanter des pratiques exemplaires dans ce milieu dynamique, même si l'on doit admettre qu'Anonymous sait bel et bien tirer les leçons du passé.

Évidemment, si tous les groupes militants évitaient l'institutionnalisation, de nombreux objectifs politiques plus larges en souffriraient. L'intellectuelle féministe Larisa Mann, qui a su dégager les forces d'un militantisme politique flexible et adapté aux circonstances, est

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

d'avis qu'«Anonymous a peut-être une longueur d'avance sur les féministes modérées dans la lutte contre la culture du viol dans les petites villes[56]». Elle précise ses propos: contrairement aux acteurs institutionnels, Anonymous (à l'instar d'autres mouvements perturbateurs éphémères) n'est pas entravé par les chaînes «de l'autopromotion et du financement», une réalité incontournable pour la quasi-totalité des associations institutionnalisées. Ces exigences peuvent endiguer le genre de réactions promptes et vives qu'Anonymous a élevées au rang d'art.

S'il y a une conclusion à tirer de ce bref tour d'horizon, c'est bien la suivante: le travail nécessaire au changement social et politique requiert – et peut supporter – une boîte à outils diversifiée, allant des interventions étatiques réglées avec précision aux tactiques subversives chahuteuses. On devrait se garder de considérer toute option comme une panacée. Si je devais faire un choix entre une ONG qui œuvre à la défense des droits des femmes et les interventions tumultueuses et problématiques d'Anonymous, j'opterais sans doute pour l'ONG. Mais cette dichotomie est un argument spécieux. La question urgente consiste plutôt à se demander comment encourager la pollinisation croisée. Ceux et celles qui poursuivent ces objectifs politiques seraient mieux avisés de chercher à forger des alliances que de formuler des critiques basées sur des différences de tactiques.

Nous avons besoin de récits captivants qui mettent en scène des enjeux autrement négligés, soutient le spécialiste des médias et militant de longue date Stephen Duncombe. Il appuie sans réserve le type de spectacle qu'offre Anonymous, et que des journalistes comme Levy rejettent en le qualifiant de fantaisie juvénile masculine[57]. Nous avons cruellement besoin de groupes bien financés, pourvus de solides équipes d'avocats, de militants et de stratèges, et disposant des ressources nécessaires à des interventions stratégiques à plus long terme. Nous avons grand besoin de journalistes d'enquête (bien payés) qui consacrent des années à traquer des sources et à emboîter les pièces de puzzles difficiles. Néanmoins, lorsqu'elles sont appliquées isolément et que leur mise en scène fait défaut, ces stratégies échouent souvent, comme nous l'avons vu avec la tragédie de Maryville. Elles ne parviennent tout simplement pas à susciter l'attention ou la volonté

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

collective nécessaires pour ébranler des mentalités et pratiques bien enracinées. Le vrai problème est ailleurs: bien des gens n’ont pas la volonté d’entrer dans l’arène politique et d’y mener une lutte, ou sont trop cyniques pour le faire.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Conclusion

Aurore

LE 6 JUIN 2013, assise dans un auditorium glacial de l'université de New York, j'attends mon tour pour prendre la parole au Personal Democracy Forum (PDF), un événement annuel destiné à souligner le rôle d'internet dans le développement de la démocratie. Je sens que je suis en train de sombrer dans le pessimisme. Mes travaux sur ceux qui percent, creusent et rongent en cherchant à rester incompréhensibles, cachés et énigmatiques (pour paraphraser les premières lignes d'*Aurore* de Nietzsche) commencent à définir un portrait plutôt sombre. Anonymous continue à bousculer l'ordre établi avec ses opérations, mais Barrett Brown, Jeremy Hammond et plusieurs autres Anons croupissent maintenant à l'ombre. Internet s'est perfectionné en une immense machine à pister. Des firmes de défense privées, des sociétés comme Facebook et les agences américaines au sigle de trois lettres (de concert avec leurs pendants des autres pays membres de l'alliance Five Eyes) ont planté leurs griffes; elles nous suivent à la trace et sont en mesure de prédire nos moindres faits et gestes. Bien que chaque organisation ou pays poursuive des objectifs différents et utilise ses propres techniques, le phénomène a pour résultat net une inquiétante limitation des droits de la personne. Anonymous, comme je m'apprête à l'affirmer dans ma conférence, est «l'invité turbulent aux funérailles de la liberté et de la vie privée en ligne».

Je ne suis pas la seule à faire ce constat peu réjouissant. L'Anon m0rpeth l'a formulé ainsi: «Quand tout sera foutu, il ne restera plus que

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

quelques petits *darknets* épars dans les marges d'internet.» Même les organisateurs du PDF, d'ordinaire emballés par la possibilité qu'internet fasse pencher la balance du pouvoir du côté de la liberté et de la justice, ont admis, lors d'un dîner offert la veille que «les choses n'ont pas pris la tournure que nous espérions».

Soudain, juste avant qu'on m'appelle à gagner la tribune, un des organisateurs du PDF, Micah Sifry, me lance une bouée de sauvetage inattendue. Il se penche, me passe son téléphone et chuchote: «Une fuite majeure sur la surveillance par l'État vient d'avoir lieu.» Je parcours un article sur l'appareil. Rédigé par le journaliste Glenn Greenwald, celui-ci révèle la collecte tentaculaire de métadonnées d'appels téléphoniques effectuée par l'opérateur Verizon pour le compte de la National Security Agency (NSA). En quelques jours seulement, Edward Snowden, le lanceur d'alerte qui a transmis l'information à Greenwald, deviendra une figure connue de tous. Sifry monte sur scène. Avant de me présenter, il apprend la nouvelle à l'auditoire. Je modifie mon exposé sur Anonymous pour y inclure ce revirement inespéré.

En démasquant la NSA (et son pendant britannique, le Government Communications Headquarters [GCHQ]), Snowden a certes pris un grand risque, mais il s'est soigneusement préparé. Ses révélations confirment les craintes soulevées depuis des années par les militants pour la protection de la vie privée; celles-ci reposeront désormais sur des preuves nettement plus solides et abondantes. Laura Poitras, une des trois premières journalistes à avoir reçu les documents de la NSA, soulignera ainsi le caractère inédit de la situation: «Les révélations de Snowden ont levé le voile sur un vaste monde occulte, où les décisions sont prises en secret et où le pouvoir s'exerce en catimini, à l'abri de toute supervision et sans le consentement de la population. Mon point de vue sur la situation n'a pas vraiment changé, mais je suis maintenant en mesure de voir beaucoup plus de choses[1].» Voici quelques exemples de ce que cette mégafuite aura révélé: la NSA a espionné ou surveillé 38 ambassades ou missions diplomatiques; jusqu'en 2011, elle a recueilli et stocké d'innombrables courriels et quantité de données en provenance des États-Unis dans le cadre d'un programme

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

appelé Stellar Wind; elle a contraint les géants des technologies à lui transmettre des données en vertu du Foreign Intelligence Surveillance Act (FISA, loi sur la surveillance et la collecte de renseignements à l'étranger), tout en en siphonnant secrètement d'autres dans des câbles de fibre optique, dont ceux de Google; elle a hacké le réseau de communication interne d'Al Jazeera; le GHCQ, lui, a mené une attaque informatique par saturation contre Anonymous et a hacké Belgacom, une société mixte de télécommunications de Belgique; dans le cadre d'un programme nommé avec à-propos Optic Nerve, il a intercepté et stocké les séquences webcam de millions d'utilisateurs de Yahoo!. Et la liste ne s'arrête pas là: au terme d'une enquête journalistique de quatre mois, Barton Gellman et Julie Tate démontreront que «les internautes lambda, qu'ils soient américains ou non, sont de loin plus nombreux à voir leurs communications interceptées par la NSA que les étrangers qui sont des cibles officielles[2]».

Étonnamment, un rapport de la NSA préparé en 2012, qui fait aussi partie des documents divulgués, fait état de l'insatisfaction de l'agence à l'égard de tous ces accomplissements. Elle souhaite élargir la portée de ses opérations par une stratégie numérique encore plus offensive qui lui permettrait de recueillir des données sur «n'importe qui, à tout moment et en tout lieu», rapportent Laura Poitras et James Risen dans le *New York Times*[3].

Ces formes invasives et systématiques de surveillance tuent dans l'œuf toute possibilité d'un «droit d'être laissé tranquille» (*right to be let alone*), pour reprendre la célèbre formule de Samuel Warren et Louis Brandeis, qui, en 1890, jetaient les bases juridiques du droit à la vie privée[4]. Et elles ne s'attaquent pas uniquement à la sphère privée, si nécessaire à la formation du sujet libéral: elles rendent aussi pratiquement impossibles des types d'association essentiels à la vie démocratique. Riseup, un fournisseur de services internet et collectif voué au changement social, résume bien la situation:

> À la base, la surveillance est une forme très efficace de contrôle social. Le fait de se savoir toujours observé modifie nos

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> comportements et étouffe la dissidence. L'impossibilité de s'associer secrètement signifie que la libre association n'est plus qu'une vue de l'esprit. L'impossibilité de chuchoter signifie qu'il n'existe plus le moindre discours véritablement libre de toute coercition, que celle-ci soit effective ou implicite. Plus fondamentalement, la surveillance généralisée menace l'élément le plus indispensable à la démocratie comme aux mouvements sociaux: l'espace mental qui permet au citoyen de se forger une opinion dissidente et impopulaire[5].

Les agences de renseignement ont évidemment besoin d'un minimum de secret pour fonctionner efficacement, dans l'intérêt du public. Cependant, si le secret échappe à tout contrôle (et en particulier s'il est le fait d'organisations disposant déjà de pouvoirs et de ressources extraordinaires), il devient un terrain propice à des dérives semblables au Counter Intelligence Program (COINTELPRO) du Federal Bureau of Investigation (FBI) sous J. Edgar Hoover.

Le dispositif de surveillance mis au jour par Snowden se distingue aussi par sa technologie – et constitue ainsi un précédent historique. Avec une puissance informatique suffisante, la collecte de données devient terriblement facile, en particulier si elle est entièrement automatisée. «Une fois assemblée la souricière que représente l'infrastructure de surveillance, on s'empressera d'en consulter les données», observe l'avocate Jennifer Granick, qui défend les libertés civiles[6].

L'État compte beaucoup sur les données recueillies et les rapports de ses informateurs pour identifier certains groupes; dans leurs activités d'espionnage actuelles, Américains et Britanniques manifestent un intérêt disproportionné pour les musulmans, les écologistes et, de plus en plus, les hackers militants[7]. C'est la conclusion à laquelle arrive un rapport préparé par trois associations de défense des droits civils et intitulé *Mapping Muslims: NYPD Spying and Its Impact on American Muslims* (Cartographier les musulmans. L'espionnage par la police de New York et ses conséquences sur les musulmans américains), qui porte sur une division de la police de New York au nom révélateur, l'«unité démographique»[8].

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Mise en place par un ancien cadre de la Central Intelligence Agency (CIA) dans la foulée du 11-Septembre, celle-ci s'est avérée si controversée et inefficace (aucun renseignement exploitable n'a été tiré des données recueillies) qu'on a fini par la démanteler en avril 2014, après qu'elle eut perturbé le tissu social des milieux ciblés pendant plus d'une décennie[9]. Le programme, qui a fait appel à 15 000 informateurs, a permis la constitution d'un vaste dossier alimenté par une surveillance vidéo et photographique à grande échelle. Un étudiant musulman cité dans le rapport a bien résumé son caractère invasif: «C'est comme si la loi disait: plus vous êtes musulman, plus vous représentez une menace, alors éloignez-vous de l'islam[10].» La fuite a aussi confirmé que la NSA surveille «d'éminents musulmans américains», dont des avocats, des professeurs et d'autres professionnels, même s'ils ne sont aucunement associés à quelque activité terroriste ou criminelle. Par exemple, de cinq personnes ayant fait l'objet d'une enquête de trois mois ponctuée d'interrogatoires minutieux, «chacune a nié avec véhémence toute implication dans des actes de terrorisme ou d'espionnage, et aucune n'a défendu le djihad avec violence ou n'est connue pour avoir participé au moindre crime, malgré des années de surveillance étroite par l'État et la presse[11]».

Aux États-Unis, les musulmans sont les premiers touchés par ce que l'American Civil Liberties Union (ACLU) qualifie de «surveillance non justifiée par des soupçons[12]». La surveillance à grande échelle a cependant des conséquences sur toute la société. «Si vous vivez en situation de surveillance pendant assez longtemps, la censure s'installe dans votre tête», affirme de façon convaincante la journaliste Laurie Penny[13]. Quand les caméras de surveillance deviennent une composante banale du mobilier urbain, quand les géants d'internet conservent des registres de la navigation et des communications en ligne des utilisateurs (et les rendent effroyablement faciles d'accès pour la NSA), et quand les gestionnaires et les patrons ont la possibilité «d'évaluer et de contrôler leurs employés comme jamais auparavant», pour citer le reporter Steve Lohr, c'est l'ensemble de la société qui en paie le prix[14]. En se superposant les uns aux autres, ces différents vecteurs de la surveillance poussent les citoyens à

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

se fondre dans la masse, à y penser à deux fois avant d'énoncer une opinion, bref, à se conformer à un ensemble restreint de normes prescrites. Le conformisme social favorise une résignation tranquille et décourage les idées, l'expression et les pratiques audacieuses (par essence risquées), nécessaires à une saine dissidence démocratique.

Parviendra-t-on, avec l'aide de gens comme cet ex-sous-traitant de la NSA qui a risqué gros en prenant la parole, à contraindre les gouvernements à juguler ces pratiques abusives et, ce faisant, à rétablir le droit de s'associer librement à l'abri de toute surveillance excessive? Les obstacles sont colossaux. Aux États-Unis, les voies normalisées du changement politique sont très étroites[15]. Avec ses serveurs centralisés et contrôlés par de grandes entreprises, l'architecture technique d'internet rend la captation des données particulièrement facile et tentaculaire, une situation que l'avocat Eben Moglen qualifie de «recette pour une catastrophe». Avec d'autres technologues, l'expert en sécurité informatique Bruce Schneier abonde dans le même sens: «Il faudra trouver le moyen de restructurer internet pour mettre un terme à cet espionnage en gros[16].» Pour le technologue maison de l'ACLU Christopher Soghoian, tant que les sociétés internet continueront de «monnayer les données personnelles de leurs utilisateurs», elles ne pourront jamais mettre en œuvre de véritables politiques «pro-utilisateur[17]» de protection de la vie privée.

Pourtant, ce paysage qu'on croyait désespérément désolé semble devenu une terre fertile. Le milieu geek politisé continue de prendre de l'ampleur, tant en nombre qu'en portée. Les diverses organisations et militants qui le composent collaborent avec des hommes et des femmes politiques, des avocats, des journalistes et des artistes. Nombre d'entre eux sont issus des recoins les plus geeks d'internet. En font partie Julian Assange, Birgitta Jónsdóttir, Chelsea Manning, Sarah Harrison, l'Electronic Frontier Foundation (EFF), les développeurs de Tor, Anonymous, Riseup, Edward Snowden et bien d'autres. Les années 2013 et 2014 ont été particulières: jamais autant de geeks et de hackers n'avaient manié leurs claviers à des fins d'expression politique, de dissidence et d'action directe[18].

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Grâce à eux, de plus en plus de gens réalisent qu'on est à la croisée des chemins. Snowden a déclenché un débat public enflammé sur la vie privée, lequel s'est poursuivi pendant plus d'un an, ce qui constitue un petit miracle dans un paysage médiatique obnubilé par la nouveauté, qui évite les discussions approfondies. Aux États-Unis, des transformations législatives encourageantes semblent poindre à l'horizon. En juin 2014, dans ce que le défenseur de la liberté d'expression Trevor Timm qualifie d'«étonnante réprimande adressée aux avocats de la NSA et à la Maison-Blanche», la Chambre des représentants a adopté une loi ambitieuse qui proscrit tout accès sans mandat aux courriels des Américains et interdit aux agences de renseignement d'installer des portes dérobées sur les appareils commercialisés, avec ou sans la complicité du fabricant[19]. La fuite a fait sentir ses effets bien au-delà des frontières des États-Unis, constate Greenwald:

> [Les documents dévoilés par Snowden] ont transformé la vision qu'avaient les habitants de la planète de la fiabilité des déclarations des responsables américains, et transformé les relations entre plusieurs pays. Ils ont radicalement modifié la vision que l'on avait du rôle du journalisme dans sa relation avec le pouvoir gouvernemental. Et, à l'intérieur des États-Unis, ils ont donné naissance à une coalition d'une grande diversité idéologique, transpartisane, qui pousse désormais à une réforme drastique de cet État de surveillance[20].

L'affaire apparaît encore plus remarquable à la lumière de la férocité avec laquelle de nombreux représentants des autorités, en particulier dans les cercles du renseignement, ont réagi au cas Snowden. Une anecdote rend bien compte de cette attitude. En 2014, pendant la Conférence sur la défense et la sécurité, à Ottawa, Melissa Hathaway, ex-directrice du groupe de travail interagences sur internet du bureau du directeur du renseignement national des États-Unis, a raconté à l'assistance qu'elle se trouvait à Tel-Aviv quand elle a appris le départ de Snowden pour la Russie en vue d'y demander l'asile politique. «Je dois vous dire que les Israéliens croient qu'on n'aurait jamais dû le laisser monter dans cet avion. Ils croient même

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

que l'avion n'aurait jamais dû atterrir», a-t-elle déclaré. Alors que se calmait l'hilarité générale qu'elle venait de provoquer, elle a eu le bon mot que voici: «Et il se pourrait bien que je partage leur point de vue.» Pourtant, même si le lanceur d'alerte est qualifié de vulgaire criminel par Washington, ses revendications politiques gagnent chaque jour en popularité. Hathaway l'a d'ailleurs elle-même admis en entamant son intervention par cette affirmation: «Nos alliés se sentent trahis, en fait. Leurs citoyens trouvent qu'Edward Snowden est un héros[21].»

Snowden a nourri un mouvement en émergence, constitué de collectifs de geeks, d'avocats, de journalistes, de cinéastes, de politiciens et d'ONG de tendances diverses. Ce mouvement s'est joint aux luttes déjà entreprises par des associations comme Fight for the Future et l'Open Technology Institute. Ses efforts ont donné lieu à grand nombre de campagnes politiques et technologiques ciblées, dont Reset the Net, une mobilisation citoyenne pour la «diffusion d'outils de protection de la vie privée résistants à la NSA» destinée à ce que ceux-ci deviennent une composante de base d'internet[22]. Des technologies comme The Amnesic Incognito Live System (TAILS, un système d'exploitation conçu pour garantir l'anonymat de ses utilisateurs), Open Whisper Systems (une association qui développe des logiciels de cryptage à code source ouvert pour téléphones portables) et LEAP (rétroacronyme pour LEAP Encryption Access Project, une association ayant pour mission de faciliter le recours aux outils de cryptage par les internautes lambda) sont financées par des citoyens et des organisations telles que la Freedom of the Press Foundation. Snowden a lui-même approuvé ces méthodes de cryptage en les qualifiant d'efficaces et de nécessaires: «Ce qu'il faut retenir, c'est que le cryptage fonctionne», a-t-il déclaré à une salle pleine lors de l'édition de mars 2014 de South by Southwest[23]. Ces technologies sont conçues pour offrir aux futures générations d'internautes un minimum de vie privée.

La Vieille Europe et le Nouveau Monde

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Peu après la première fuite de documents de la NSA, l'Irlande a connu son premier procès dans une affaire de hacking. En juillet 2013, deux membres de LulzSec et d'Anonymous, Donncha O'Cearbhaill et Darren Martyn, ont été jugés pour le défaçage du site web du parti Fine Gael perpétré en 2011. En route vers le tribunal de Dublin, je perdis mon chemin: dépourvue de tout dispositif personnel de pistage (ou de téléphone portable, si vous préférez), je fis ce que les gens ont fait pendant des siècles, soit consulter une carte en papier, que... j'ai mal interprétée. Je mis encore quarante-cinq minutes à trouver le bon palais de justice.

Une fois sur place, j'étais convaincue d'avoir manqué le procès. Or les deux causes s'inscrivaient en fait dans une séquence de plus d'une dizaine d'audiences pour des délits mineurs, O'Cearbhaill et Martyn ne comparaîtraient donc pas avant une heure. Avec mon voisin, un Anon irlandais surnommé Firefly, nous nous sommes amusés à observer la juge (une femme avisée et corpulente dans la cinquantaine) réprimander avec bienveillance (mais fermeté) les autres prévenus. La plupart d'entre eux étaient accusés de méfaits ou d'inconduites typiquement juvéniles, comme cette jeune femme dans la vingtaine, aux cheveux noirs étonnamment longs, à l'air renfrogné, aux bras croisés et à l'accoutrement impudique, jugée coupable d'avoir agressé un membre de la Garda Síochána (police irlandaise) alors qu'elle était en état d'ébriété avancée.

Les deux causes d'Anonymous se démarquaient nettement de cette série de rixes et d'infractions attribuables à l'ivresse. Après avoir entendu les deux parties dans deux affaires de défaçage, la juge accueillit l'affirmation de la poursuite (selon laquelle le rétablissement du site web de Fine Gael aurait coûté cher) avec scepticisme. Elle demanda comment la facture avait pu s'élever à 10 000 euros si rien n'avait été endommagé, question à laquelle le procureur ne put répondre. La juge conclut que l'opération de hacking «visait à embarrasser un parti politique, et non à divulguer des données en vue de les rendre publiques». Elle ne souhaitait pas, par conséquent, l'incarcération d'O'Cearbhaill et Martyn pour avoir commis l'équivalent numérique d'un graffiti; mais elle ne considérait pas

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

pour autant leur geste comme louable. Elle les sermonna, évoquant un «terrible gaspillage de talent», puis les condamna à 5 000 euros d'amende chacun, à payer avant le mois d'octobre (la moitié des sommes devaient être versée à des organismes de charité). Ils durent également s'inscrire à un programme de justice réparatrice. Aux yeux de cette juge, le geste condamnable n'avait rien de politique... sinon, sans doute leur aurait-elle infligé une sanction encore plus clémente.

Au terme du procès, O'Cearbhaill et Martyn quittèrent les lieux avec leurs familles. Firefly et moi nous sommes dirigés vers le centre-ville pour une promenade au soleil le long du canal principal de Dublin (l'Irlande vivait depuis deux semaines une vague de chaleur miraculeuse). Nous sommes revenus sur le procès, tous deux d'avis que les Anons s'en étaient tirés avec des sentences très légères. La justice irlandaise, comme la justice britannique, se montre indéniablement plus indulgente que les tribunaux américains dans des causes comparables. Certes, le défaçage d'un site web ne se compare en rien aux actes d'un Hammond. Par contre, la longue série d'opérations de hacking perpétrées avec LulzSec par le Britannique Ryan Ackroyd, dit Kayla, s'en rapproche davantage; or, en mai 2013, après qu'il eut plaidé coupable à un chef d'accusation de conspiration en vue de hacker le Pentagone, Sony, le système de santé publique britannique et la société News International de Rupert Murdoch, un tribunal britannique a condamné Ackroyd à trente mois de prison (dont dix ont été purgés). Détail important: il n'a écopé d'aucune amende. Dans les procès intentés aux États-Unis, même lorsque les peines de prison infligées sont relativement brèves, les amendes dont elles sont assorties assurent pratiquement aux condamnés des années de servitude. À l'âge de 22 ans, John Anthony Borell III, dit Kahuna, membre de CabinCr3w, a été condamné à 26 mois de prison pour avoir hacké de nombreux sites web de services policiers et en avoir soutiré des données personnelles. Lorsqu'il aura purgé sa peine, il devra encore verser près de 230 000 dollars en dommages et intérêts.

De plus, bon nombre des accusations portées contre des hackers aux États-Unis semblent surgir de nulle part, comme en fait foi le calvaire enduré par Barrett Brown. Le 6 mars 2012, soit le jour même où Fox a

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

démasqué Sabu et où le FBI a arrêté Hammond, la police fédérale a exécuté un mandat de perquisition à la résidence de Brown. Entre autres choses, les autorités espéraient y dénicher «des données relatives à HBGary, à Infragard, à Endgame Systems, à Anonymous, à LulzSec, à des séances de chat sur Internet Relay Chat (IRC), à des billets Twitter, à wiki.echelon2.org et à pastebin.com[24]». Six mois plus tard, en septembre, le FBI a arrêté Brown (en pleine séance de communication vidéo!). En toute franchise, il faut admettre que le hacker l'avait bien cherché; il avait posté une vidéo, dont on pourrait traduire le titre par «Pourquoi je m'apprête à détruire l'agent Robert Smith du FBI, troisième partie, la revanche de l'agile», où il se livrait à une diatribe hyperbolique contre un policier fédéral qui avait interrogé sa mère[25]. Comme il fallait s'y attendre, on l'a arrêté pour menace contre un agent du FBI. Seul un extrait de son brûlot peut nous aider à mieux comprendre pourquoi il était à ce point en colère – et pourquoi le FBI n'avait d'autre choix que de l'arrêter (au lieu de considérer sa vidéo comme une banale performance artistique):

> Devinez ce qui est écrit sur ma saloperie de mandat de perquisition: fraude! J'ai pas détourné de fonds. [...] Une putain d'accusation de fraude pour un putain de militant de la plume sans le sou qui a dépensé tout son fric en frais d'avocat pour lui-même et sa putain de mère. [...] L'agent Smith a publié les adresses [de ma maison et de celle de ma mère]. [...] Smith est un criminel impliqué dans une conspiration criminelle. [...] C'est pourquoi sa vie est finie. Quand je dis que sa vie est finie, je ne dis pas que je vais le tuer, mais que je vais ruiner sa vie et m'intéresser à ses mioches. [...] Ça vous la coupe, hein? Comme l'a constaté Smith, je suis menacé par les extraterrestres. [...] Je le remercie donc [d'avoir balancé mon adresse]. [...] Parce que les extraterrestres prennent souvent l'apparence d'agents de sécurité mexicains [et sont souvent des] représentants des autorités, je crains qu'on soit en train de me jouer le même tour. [...] Le FBI, en particulier [...], peut être considéré comme une escouade d'assassins. Le FBI sait que je suis armé, que je viens d'une famille de

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> militaires, qu'un vétéran du Vietnam m'a appris à tirer [...] et que je vais tous leur tirer dessus et les tuer s'ils viennent et font quoi que ce soit, parce qu'ils sont impliqués dans une conspiration criminelle et que j'ai des raisons de craindre pour ma vie, non seulement à cause des extraterrestres, mais aussi du gouvernement des États-Unis. [...] Je n'ai d'autre choix que de me défendre, de défendre ma famille [...] et, honnêtement, vous savez, j'ai toujours été convaincu que je mourrais avant d'avoir 40 ans, alors ça me serait égal d'être tué par deux armes de poing du FBI comme un foutu pharaon égyptien. *Adios.*

À ces accusations de menaces s'ajoutèrent des inculpations liées à l'opération de hacking contre Stratfor. Dans le salon de discussion de Project PM, Brown avait partagé un lien vers un fichier hébergé sur un autre site, lequel contenait les numéros de carte de crédit subtilisés à Stratfor. Pour cette raison, il a dû répondre de dix chefs d'accusation de vol d'identité qualifié et de deux chefs de fraude par carte de crédit, des infractions qui, combinées, sont passibles de quarante-cinq ans de prison (plus une soixantaine d'années pour les autres accusations). Bien des gens ayant aussi partagé le lien n'ont pas été accusés. Le journaliste Adrian Chen, d'ordinaire assez critique envers Anonymous, écrivit: «Pour un journaliste qui couvre le milieu hacker et a "partagé et publié" de nombreux liens vers des données volées par des hackers (afin de les inclure dans des articles sur leurs opérations), une telle inculpation est terrifiante, car elle semble criminaliser le partage de liens[26].»

Parce que Brown, en se faisant le visage d'un collectif qui se voulait sans visage, causait à Anonymous tout l'embarras qu'on sait, il était loin de faire l'unanimité chez les Anons. Néanmoins, ces derniers se rangèrent derrière cette déclaration de Kevin Gallagher, l'administrateur système qui prit la direction de la campagne de soutien à Brown: «c'est son travail journalistique cherchant à faire la lumière sur des zones que les puissants préféreraient laisser occultes qui a fait de lui une cible[27]». Les défenseurs de Brown ont donc collecté des fonds, l'ont aidé à s'offrir les services d'avocats chevronnés et ont tenté de faire connaître son cas au grand public.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Dans un retournement inattendu, l'État abandonna les accusations de partage de liens deux jours à peine après le dépôt d'une requête en irrecevabilité par la défense. (Ce faisant, les autorités évitaient un dangereux précédent et se donnaient la possibilité de poursuivre des enquêtes du même acabit.) En avril 2014, risquant toujours d'être condamné à des décennies de prison, ne pouvant s'adresser aux médias et ayant déjà passé plus d'un an et demi en détention, Brown accepta une négociation de peine. En vertu de celle-ci, sa sentence potentielle ne pourrait dépasser huit ans d'emprisonnement, et il ne plaiderait coupable qu'à trois chefs d'accusation: complicité après le fait (pour le hacking de Stratfor), obstruction à un mandat de perquisition pour avoir caché des ordinateurs portables sous l'évier se sa cuisine, et menaces contre un policier fédéral.

On doit retenir une chose de cette histoire. Que l'on décide de hacker en toute impunité et dans l'anonymat (avec ou sans objectifs politiques) ou en vue de se forger une réputation d'agitateur chevronné, il vaut mieux le faire du côté européen de l'Atlantique (où Anonymous et d'autres types de militantisme geek sont plus courants).

Mais revenons en Irlande. Plus tard, dans la soirée, alors que j'étais impatiente de recueillir les impressions d'O'Cearbhaill sur le procès, ce dernier se révélait introuvable. J'apprendrais plus tard que la Garda l'avait attendu à la sortie du palais de justice pour l'arrêter derechef, mais, cette fois, pas pour une affaire de hacking. Étudiant en chimie, O'Cearbhaill disposait d'un laboratoire chez ses parents. Or, certaines des substances qui s'y trouvaient pouvaient (en théorie) servir à la fabrication d'explosifs. Même si aucune preuve n'indiquait qu'il les utilisait ou entendait les utiliser à de telles fins, on l'avait arrêté en vertu de la loi antiterroriste irlandaise.

Les procureurs ont fini par établir que la preuve était insuffisante pour que des accusations fussent portées, mais des Anons émirent l'hypothèse que la Guarda cherchait à intimider O'Cearbhaill pour lui faire admettre sa participation à une opération de hacking devenue légendaire. En février 2012, AntiSec avait en effet diffusé des fichiers audio issus d'une conférence téléphonique entre des représentants du FBI, de Scotland Yard et

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

de la Garda. La discussion portait sur nul autre qu'Anonymous. La fuite avait été provoquée pour le seul plaisir du *lulz*, mais semblait avoir mis ses victimes dans l'embarras, en particulier la Garda. C'est par l'entremise du compte de courriel d'un policier irlandais que les hackers avaient pu obtenir les données nécessaires au repérage du fichier de l'appel. (Au moment où j'écris ces lignes, personne n'a été jugé coupable de cette intrusion.)

Cette affaire laisse entrevoir une autre raison à l'hostilité des forces policières à l'égard des spéléologues de l'informatique. Les hackers se donnent parfois pour mission de «surveiller les surveillants». Kevin Poulsen et Kevin Mitnick l'ont déjà fait. Selon le spécialiste des médias Douglas Thomas, qui s'est penché sur leurs cas, «Poulsen a hacké les systèmes du FBI et y a découvert un ensemble de programmes d'écoute et de surveillance destinés à épier tout ce qui bouge, du restaurant situé en face de chez lui à (prétendument) Ferdinand Marcos[28]». AntiSec a fait la même chose, mais de façon plus visible.

Quelques jours plus tard, O'Cearbhaill s'est joint à nous pour un pique-nique estival au parc St. Stephen's Green. J'y avais réuni des Anons de différents réseaux et aux parcours opérationnels variés, de l'ex-scientologue Pete Griffiths (un fier partisan d'Anonymous) à David de l'opération Chanology, en passant par Firefly d'AnonOps et d'autres hackers comme O'Cearbhaill. Ce dernier m'en a appris un peu plus sur ce qui l'avait amené au hacking militant à l'âge de 15 ans, et sur l'engagement de son père dans l'Armée républicaine irlandaise (IRA). Ayant passé six ans en prison et mené une grève de la faim de quarante-quatre jours, celui-ci, contrairement à la juge, avait saisi spontanément les motivations politiques de son fils. En cet été 2013, j'étais d'ailleurs convaincue que la plupart des Anons sont animés d'intentions politiques; leurs activités provoquent certes des dommages, mais ils les mènent dans le but de faire poindre l'aurore, de mettre fin au sombre règne de l'injustice. On perçoit les choses autrement après avoir entendu des histoires comme celles qu'O'Cearbhaill m'a racontées. Les ombres fuyantes deviennent tangibles, intelligibles; on comprend que chaque membre possédait une riche expérience de vie au

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

moment d'adhérer à Anonymous, et que le collectif lui a ouvert de nouvelles portes.

D'ailleurs, un an plus tard, je suis retournée à Dublin où, avec 50 autres personnes, je me suis installée dans le musée des sciences de l'université Trinity pour écouter O'Cearbhaill, devenu porte-parole du Parti pirate à l'université de Dublin, donner une conférence sur Tor, l'outil de protection de la vie privée. Le rassemblement était organisé par CryptoParty, une association citoyenne née en 2012 (à l'initiative d'Asher Wolf et d'autres geeks) s'étant donné pour mission d'enseigner la cryptographie au grand public. Quelques jours après l'événement, autour d'une bière dans un pub de Londres, Mustafa Al-Bassam (tflow) m'a raconté son stage à Privacy International, la plus importante ONG européenne vouée à la lutte pour le «droit au chuchotement». Et il existe des dizaines d'autres exemples de cette tendance. Quoi qu'on pense d'Anonymous, on ne peut nier son rôle de porte d'entrée vers le politique. Après avoir quitté le collectif, nombreux sont les Anons qui continuent à contribuer à la vie politique de différentes façons.

Contrairement à Al-Bassam et à beaucoup d'autres Anons, Hammond et Monsegur étaient déjà des militants avant d'adhérer à Anonymous. Mais leurs routes ont pris des directions radicalement différentes au terme de leur engagement au sein du collectif. Peu après la révélation de sa collaboration avec les autorités, Monsegur s'est évaporé dans la nature; personne n'a eu longtemps la moindre idée de l'endroit où il se trouvait. On a fini par apprendre qu'il avait passé un peu plus de sept mois au centre correctionnel métropolitain de New York, la prison même où Hammond a été incarcéré avant d'être transféré dans le Kentucky pour purger sa peine de dix ans. C'est une source d'Anonymous qui m'a d'abord donné l'info, et mes demandes répétées à des journalistes pour une enquête en bonne et due forme sont restées vaines. Beaucoup plus tard, j'en ai obtenu la confirmation, de la part de Hammond lui-même. Le 26 mai 2014, quand Monsegur a enfin reçu sa sentence après sept reports, les causes de sa seconde arrestation et de son incarcération ont été rendues publiques. Le hacker avait dérogé aux conditions de sa caution en publiant un billet de

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

blog et en chattant avec un membre d'Anonymous. Au moment de prononcer sa sentence, la juge Loretta Preska s'est lancée dans un éloge vibrant de Monsegur, qu'elle a qualifié d'informateur modèle dont le séjour de 2012 en prison avait constitué une peine suffisante. Sabu était désormais un homme libre. Avant qu'il ne quitte le tribunal, la juge Preska a poursuivi ses louanges: «La coopération immédiate et constante de M. Monsegur s'est avérée particulièrement utile pour l'État. [...] Sa capacité à faire volte-face en vue de faire le bien au lieu du mal est le facteur qui a le plus contribué à la détermination de cette sentence.» Par sa clémence, Preska a transmis de façon peu subtile le message suivant aux futures taupes: si vous collaborez, vous serez bien traité.

Malgré cet aboutissement somme toute sans surprise, un tollé a déferlé sur Twitter: «Jeremy Hammond purge une peine de dix ans pour des opérations de hacking que Sabu (qui travaillait pour le FBI) lui a demandé de mener?» a demandé @YourAnonNews[29]. «Preska fait honte à la notion de justice», a lancé Firefly dans une interview. Ces lamentations n'ont rien changé au triste sort de Hammond, mais de nombreux Anons ont éprouvé un certain réconfort quand, à peine quelques jours plus tard, les webmagazines *Motherboard* et *The Daily Dot* ont publié des reportages qui remettaient en question la version des autorités – et corroboraient celle de Hammond. En plus d'offrir sa collaboration «constante», Monsegur avait eu le champ libre pour proposer et coordonner des dizaines d'opérations de hacking, rapportaient les articles.

À la suite de la libération de Monsegur, Hammond a publié une déclaration:

> En poursuivant activement des hackers qui obéissent à leurs propres règles, les autorités souhaitent dissuader la relève et espèrent que de nouvelles arrestations leur procureront de nouveaux collaborateurs en herbe. Nous devons continuer de refuser les justifications visant à rendre acceptable le fait de vendre ses amis et de devenir un pion du cyberimpérialisme. [...] Sabu a évité la prison, mais les conséquences de ses gestes le hanteront pour le reste de ses jours. Je n'ai pas encore

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

> purgé la moitié de ma peine, mais je préfère tout de même ma situation: ils peuvent me priver de ma liberté pour un temps, mais mon honneur, lui, durera éternellement[30].

Ce long séjour en prison sera assurément éprouvant pour Hammond, mais son inébranlable fidélité à ses principes, malgré la révélation de son identité et son incarcération, est déjà une source d'inspiration pour de nombreux militants.

Certains trouveront sans doute insolite de voir une chercheuse se mêler à ce point à son objet d'étude, mais c'est depuis longtemps la norme en anthropologie. Comme l'explique Danilyn Rutherford, la méthode anthropologique «entraîne des obligations, obligations qui contraignent les chercheurs à prendre des risques en faisant des affirmations qui influent sur le contexte et les groupes qu'ils étudient[31]». Dans le cadre d'une campagne de lettres d'appui organisée par les avocats de Hammond, j'ai écrit, avec 150 autres personnes, à la juge Preska pour implorer sa clémence; dans nos lettres, nous soulignions la nature politique d'Anonymous. Chaque fois que l'occasion se présente, je tente de rendre l'univers déroutant du collectif intelligible à des publics divers. J'ai aussi écrit des lettres à des Anons emprisonnés. Mes obligations d'anthropologue m'ont amenée à réfléchir en long et en large aux finalités sous-jacentes du projet de recherche à l'origine de ce livre. J'ai fini par comprendre que je poursuivais deux objectifs contradictoires: réfuter les informations erronées et cultiver l'émerveillement.

En écrivant ce livre, j'ai avant tout voulu dissiper les préjugés infondés qui entourent Anonymous: de nombreux participants comme O'Cearbhaill ne sont pas motivés principalement par le *lulz*, même si cet esprit irrévérencieux persiste à guider les interactions sociales et à donner le ton aux stratégies du collectif. En mûrissant, Anonymous est devenu un mouvement politique sérieux, à tel point que beaucoup de trolls de l'époque de la «machine de haine d'internet» «ne reconnaissent plus» le collectif actuel, affirme Ryan Ackroyd. Ce dernier fait partie de la poignée d'Anons qui ont connu ces deux époques maintenant considérées comme distinctes.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

(Bien entendu, cela ne signifie pas que la machine de haine ne se manifestera pas de nouveau, comme l'a tweeté un Anon surnommé blackplans: «Sans les trolls, les hackers et les hordes de 4chan, qui des personnes aimables et sensibles que vous êtes auraient entendu parler d'Anonymous? Gardons ça en mémoire[32].»)

Dans le cadre de cette première mission que je me suis donnée, j'ai voulu éviter d'encenser tous les faits et gestes d'Anonymous. Même dans ses incarnations militantes, le collectif s'est livré à des activités indéniablement douteuses – et parfois carrément odieuses – sur le plan moral. Les épisodes les plus troublants sont ceux où des innocents tombent sous les rafales des Anons. Certaines opérations m'ont frappée par leur caractère contre-productif ou parce qu'elles n'étaient pas à la hauteur des risques pris par ceux et celles qui y prenaient part. Certains éléments constitutifs d'Anonymous sont d'ailleurs pétris de contradictions insolubles.

C'est pourquoi il me semble aujourd'hui impossible de rendre compte de l'impact qu'a Anonymous sur la société en une formule simple et univoque. J'ai plutôt tenté de faire part des leçons qu'a tiré le collectif de ses hauts faits, de ses échecs et de ses succès. Ces récits sont idiosyncrasiques, et je les ai racontés de mon propre point de vue. Du reste, les histoires secrètes ou inconnues sont incalculables, et leur dévoilement changerait sans doute la perception qu'on peut avoir d'Anonymous. La vie sociale et les mouvements politiques sont déjà des réalités complexes aux innombrables facettes et dimensions; et Anonymous, avec son penchant pour la multiplicité, le secret et la tromperie, ne cède pas sa place.

Cette multiplicité et ce dynamisme sont aussi une des grandes forces du collectif. En ce sens, il est représentatif d'un certain type de résistance, celle qui émane d'une nébuleuse faite d'un grand nombre de groupes concurrents. Le pouvoir peut s'y imposer pendant un temps, mais la domination à long terme par un groupe ou un individu en particulier y est pratiquement impossible. Dans un contexte aussi dynamique, il est «facile de récupérer, mais impossible d'être récupéré», comme l'a habilement constaté Quinn Norton lors d'une table ronde à South by Southwest en mars 2013. La «nature» multiple d'Anonymous empêche son assujettissement

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

par d'éventuels ambitieux issus de ses propres rangs ou par des forces externes qui viendraient l'influencer avec des taupes comme Sabu ou en faisant pression autrement. Insondable, Anonymous nous force à nous contenter des fragments qu'il daigne nous laisser voir.

Anonymous laisse une grande place à l'imagination. Mais pas toute la place: il est essentiel de comprendre comment le collectif est passé d'une bande de trolls sinistres à un groupe d'activistes assumant un rôle public, d'autant plus que l'État (procureurs, gouvernements et juges en tête) présente ses membres comme de vulgaires criminels. Ces représentants des pouvoirs en place refusent d'admettre que les actions d'Anonymous découlent d'un élan militant. D'ailleurs, c'est sans doute en raison de la force et du caractère politique des actions d'Anonymous que les autorités sont si promptes à criminaliser les Anons[33].

Ainsi, même si j'ai tenté de faire tomber les idées reçues, la perspective de dissiper complètement l'aura de mystère et de magie entourant Anonymous m'a semblé inacceptable (si elle est possible). Pour la philosophe Jane Bennett, nous devrions «résister au désenchantement de la modernité» et «accroître l'enchantement»[34]. Voilà qui résume bien le second objectif que j'ai poursuivi en recueillant ces récits captivants. Le fait de délibérément accorder de la valeur à l'enchantement, affirme Bennett, est un geste politique significatif. Un geste que je suis déterminée d'accomplir (pour des raisons qui deviendront plus claires dans ces dernières pages).

Au vu de ce second objectif, il allait de soi, pour moi, de frayer avec la mythologie, et d'embarquer le *trickster* dans l'aventure. Les personnages présentés dans ce livre incarnent les contradictions et les paradoxes de la vie, dont bon nombre sont insolubles. Des leçons se dégagent de leurs histoires, non pas sous la forme de sermons rigides, mais plutôt à travers le récit de leurs exploits, fascinants et souvent audacieux. De toute évidence, les us et coutumes des *tricksters* relèvent du mythe, mais on ne doit pas oublier qu'ils ont été, à un moment donné, façonnés par des mains humaines. Mon rôle a consisté à montrer ce processus de création de mythes historiques et politiques, processus évidemment à l'œuvre pour une

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

entité constituée d'artistes de talent, de créateurs de mythes contemporains et de fabricants d'illusions.

Maintenant que la fin du voyage approche et que j'ai exposé les objectifs qui ont guidé mon travail, c'est à vous, lecteur, de juger si j'ai su équilibrer les forces apolliniennes de l'empirisme et de la logique avec les forces dionysiaques de l'enchantement. Quoi que vous en pensiez, je vous prie de m'autoriser à vous faire part de mes réflexions ultimes, où j'explore les zones encore noires et en survole d'autres déjà copieusement garnies de broderies. Bien qu'Anonymous me laisse encore souvent perplexe, j'ai pu récolter une série de messages exaltants dans son sillage.

Anonymous Everywhere

Malgré sa structure et sa nature insaisissables, Anonymous est constitué d'individus qui décident, ensemble et séparément, de prendre position. Qui peuvent bien être ces gens? Un voisin? Une jeune fille? Une secrétaire? Un concierge? Une étudiante? Un bouddhiste? Un banquier qui agit incognito? Quel que soit leur profil, une chose est sûre: cette entité, qui a vu le jour en tant que réseau de trolls, s'est métamorphosée en un foyer de résistance sur le net. Après sa campagne contre l'Église de scientologie, le collectif a élargi ses horizons pour englober un échantillon mondial de causes politiques allant du combat contre la censure en Tunisie à la dénonciation des injustices économiques et politiques au parc Zuccotti et à la place Tahrir, en passant par la lutte contre la culture du viol en Amérique du Nord.

Malgré son rapport imprévisible (pour ne pas dire irrévérencieux et souvent destructeur) à la loi, Anonymous offre une illustration de ce que le philosophe de l'école de Francfort Ernst Bloch appelle «le principe espérance». Après avoir fui l'Allemagne nazie, Bloch s'est réfugié aux États-Unis, où il a écrit un traité en trois volumes sur le sujet. Animé d'une intention «encyclopédique», il a répertorié un ensemble de signes, de symboles et d'objets très divers ayant véhiculé l'espoir à différentes

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

époques. Ses exemples vont de ses propres fantasmes aux contes de fées immémoriaux, en passant par l'amour de la musique et des sports ou encore les traités mystiques ou philosophiques – bref tout ce qui peut allumer ou transmettre l'étincelle de l'espoir. Rédigée dans l'ombre d'un courant particulièrement pessimiste du marxisme, l'œuvre de Bloch rappelle qu'un monde meilleur – ou à tout le moins l'intuition de ce que le monde pourrait être – est déjà parmi nous. En se livrant à une forme d'archéologie philosophique, Bloch a déterré des signes d'utopie capables de combattre l'«angoisse» et la «crainte» chez quiconque en prend conscience. «L'affect de l'espoir sort de lui-même, agrandit les hommes au lieu de les diminuer [...]. Le travail de cet affect réclame des hommes qu'ils se jettent activement dans le devenir, dont ils font eux-mêmes partie», écrit-il[35]. À mes yeux, le fait qu'un militantisme politique solide ait pu émerger des bas-fonds les plus sordides d'internet (que des geeks se soient activement engagés dans un processus de politisation) s'inscrit parfaitement dans ce principe de l'espérance.

Pour Bloch, «l'espoir menteur est un des plus grands malfaiteurs[36]». Celui-ci se caractérise par son optimisme aveugle et son incapacité à catalyser un mouvement. L'espoir que défend le philosophe est plutôt de nature inquiète, fondé sur la passion, l'émerveillement et même la malice – des qualités auxquelles adhère Anonymous. Voilà qui fait ressortir la dimension fortement positive de l'esprit du collectif, un élan vers une forme réaliste d'espoir qui, lorsqu'elle se manifeste, semble capable d'induire des bouleversements et des transformations. Les Anons n'ont évidemment pas le monopole de ces formes de passion et d'espoir, mais, à part chez une poignée de penseurs éminents comme Chantal Mouffe ou Jacques Rancière, le caractère émotionnel de la vie politique est souvent relégué à la marge – ce qui est curieux vu la place centrale qu'occupent le désir et le plaisir dans sa nature même. Il y a cependant d'autres raisons, plus cruciales que la simple réparation de l'omission d'une composante aussi fondamentale du militantisme, de souligner les facteurs émotionnels qui sont partie intégrante du processus de changement social.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

En 2008, quand la redoutable bande de trolls qu'était alors Anonymous a entrepris un virage à gauche décisif en rompant avec le «salopage sur internet ultracoordonné» et en se lançant dans le militantisme, elle a surmonté un des sentiments dominants de notre époque. Le spécialiste des médias Whitney Phillips affirme avec éloquence que la période historique actuelle est imprégnée d'un cynisme généralisé, et que les trolls représentent un des extrêmes les plus denses et les plus grotesques d'une sous-culture fondée sur la dissociation émotive (ou le fétichisme politique) [37].

De nombreux théoriciens et écrivains issus de traditions très éloignées les unes des autres, allant du romancier américain David Foster Wallace à l'autonomiste italien Franco Berardi, dit Bifo, soutiennent que le cynisme est devenu le prisme à travers lequel une bonne partie des Nord-Américains et des Européens perçoivent et interprètent le monde. Wallace aborde la généralisation «de l'inquiétude passive et du cynisme» et appelle «les antirebelles et les badauds nés» à se soulever et «à oser prendre leurs distances d'avec leur regard ironique sur le monde»[38]. Après avoir écrit de nombreux ouvrages sur le sujet, Bifo s'est tourné vers la poésie pour traiter du terrible fardeau émotif du cynisme:

> *Avant que le tsunami ne frappe, vous savez ce qui se passe?*
> *La mer recule, laissant un désert mort où seuls subsistent le cynisme et l'abattement.*
> *Vous n'avez alors qu'à vous assurer d'avoir les bons mots à dire et les bons vêtements à porter avant qu'il ne vous emporte*[39].

Le sentiment de découragement est comparable à des chaînes, et pas seulement au sens figuré. Même lorsque les citoyens sont conscients des forces qui les escroquent, le cynisme peut empêcher tout changement politique. En se répandant, cet état d'esprit gangrène les forces vives de la société, ce qui amplifie la fragmentation, étouffe la solidarité sociale et limite considérablement les potentialités politiques[40]. En ajoutant l'anxiété au mélange, il en résulte un cocktail des plus toxique. Le collectif britannique de gauche Plan C a publié un pamphlet clairvoyant intitulé «We

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Are All Very Anxious» (Nous sommes tous très anxieux). Ses auteurs y font des liens entre les conditions économiques difficiles, la précarité de l'emploi, les arrestations préventives de militants, l'importance de l'autopromotion dans la culture contemporaine et la réalité implacable des dispositifs de surveillance: «L'omniprésence et les multiples facettes du réseau de surveillance sont une des principales causes sociales de l'anxiété. [...] Mais ce réseau visible ne représente que la surface. [...] L'exposition de soi volontaire et ostentatoire par l'entremise des médias sociaux, de la consommation et du choix d'une position dans le domaine de l'opinion joue aussi un rôle actif en ce qui concerne le regard continuellement posé sur soi par un autrui virtuel[41].» Quand on ajoute à cette dérive vers la mise en place d'un panoptique la litanie de grands enjeux que sont la croissance des inégalités, les vagues de récession et d'instabilité et les sombres perspectives environnementales liées au changement climatique, on comprend aisément comment une incertitude handicapante, envahissante et terrifiante a pu se répandre.

Le cynisme et l'anxiété sont peut-être généralisés, mais ils ne sont ni omnipotents ni omniprésents; ils se butent chaque jour à une certaine résistance. D'innombrables militants, immigrants, déplacés, réfugiés, inconnus et artistes – ainsi que, chose remarquable, certains hommes et femmes politiques – sont en lutte contre l'oppression et cherchent à repousser l'attaque émotionnelle qui enferme si facilement les gens dans de tels pièges existentiels. On doit prendre garde de brosser un portrait trop sombre de la situation et d'ajouter ainsi au cynisme et à l'anxiété mêmes qu'on cherche à éliminer. Bloch nous presse de contribuer à des archives vivantes de l'espoir, d'être attentifs «à bien autre chose qu'aux litanies funèbres d'un monde nihiliste voué au néant et oppressé jusqu'à l'étouffement[42]».

En tenant compte du fait que les Anons connaissent bien cette condition, il apparaît d'autant moins surprenant – ou d'autant plus surprenant – qu'ils aient su contribuer à ces «archives vivantes de l'espoir». Je suis incapable de déterminer si Anonymous attire des gens naturellement sombres, ou si ce milieu pseudonyme est simplement propice au partage de

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

ce qui relève de facettes universelles de la condition humaine. Il est probable que la réalité soit un peu des deux. Mais j'ai souvent été frappée par cette association entre douleur existentielle et désir ardent d'en venir à bout.

En se dispensant de personnalités publiques, en évitant d'avoir des chefs et, par-dessus tout, en refusant le jeu de l'autopromotion, Anonymous s'entoure de mystère, ce qui est en soi un geste politique radical dans un ordre social fondé sur la surveillance systématique et la glorification de l'individualisme et de l'égoïsme. L'iconographie du collectif (le masque et le costume sans tête) souligne visuellement l'importance de cette opacité. Anonymous n'est peut-être pas la ruche que le collectif prétend être ou qu'on imagine – et est sans doute déchiré par des querelles internes –, mais il offre tout de même un portrait saisissant de la solidarité – *e pluribus unum* (de la diversité dans l'unité, la devise des États-Unis).

«Une flamme vacillante exige des soins constants, un feu de camp peut être laissé à lui-même, un brasier s'étend», disait l'Anon papersplx. En adoptant le masque, qui, comme le rappelle le sociologue Richard Sennett, «est un des accessoires culturels les plus anciens, rattachant la scène et la rue[43]», Anonymous s'est approprié la dynamique du travestissement et l'a transférée d'internet à la résistance au quotidien. Le collectif est devenu un symbole de dissidence, un moyen de canaliser le profond désenchantement provoqué par un dictateur, une loi, l'économie, la culture du viol – en gros, par quoi que ce soit. Anonymous, c'est celui qui n'hésite jamais à prendre des risques, qui aime jouer avec le feu, quitte à s'embraser (nombreux sont les Anons qui se moquent des mesures de sécurité), ouvrant ainsi la voie aux autres. Des gens se brûlent, tant chez les hackers que parmi leurs cibles. «C'est comme un phénix. Il lui arrive de prendre feu et de se consumer entièrement, mais il renaît de ses cendres, plus fort que jamais», lance Firefly dans le documentaire *We Are Legion*[44]. En transgressant systématiquement les règles et les limites, les Anons risquent souvent leur liberté, mais, avec son principal mot d'ordre (tout le monde est libre d'agir au nom d'Anonymous), le collectif favorise sa résurrection et sa réinvention.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

À maintes reprises, Anonymous m’est apparu comme une vision déconcertante, éblouie que j’étais par la lumière vive de ses rêves merveilleux (et choquants, et troublants). C’est cette capacité d’être à cheval entre l’espace du mythe et la réalité militante du risque propre à l’action directe qui rend le collectif si séduisant. En prenant un certain recul, on a l’impression d’observer des aurores boréales, une bataille mythique entre dieux et *tricksters* dans le ciel nocturne, un ciel d’autant plus enchanteur qu’il peut être contemplé par tout le monde. Le pouvoir de l’anonymat éponyme d’Anonymous réside dans la liberté que nous avons tous de porter ou non le masque.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Épilogue

L'état d'Anonymous

De plus en plus, j'aime le secret. C'est, je crois, la seule chose qui puisse nous rendre la vie mystérieuse ou merveilleuse. La chose la plus banale devient délicieuse dès l'instant qu'on la dissimule.

Oscar WILDE

La culture politique des techniciens apolitiques est extraordinaire.

Julian ASSANGE

LA PÉRIODE SUR LAQUELLE se penche se livre représentera sans doute, pour beaucoup de gens, celle de l'apogée d'Anonymous – en font foi le soutien apporté par les Anons à divers mouvements constitutifs du Printemps arabe, la grande attention médiatique suscitée par les opérations de hacking audacieuses de LulzSec et d'AntiSec, ou l'intérêt croissant du collectif pour les questions de justice sociale dont ont témoigné ses campagnes contre la culture du viol et la brutalité policière.

Toutefois, comme on pouvait s'y attendre, cette remarquable effervescence d'activités contestataires a donné lieu à une répression impressionnante. En Europe, en Asie, en Australie et dans les Amériques, les autorités ont incarcéré plus d'une centaine de militants d'Anonymous, dont certains, comme Jeremy Hammond et John Anthony Borell III aux États-Unis, ainsi que Ryan Ackroyd et Mustafa Al-Bassam au Royaume-Uni, ont eu une place importante dans ce livre. Parmi les autres arrêtés se trouvent des geeks dont le seul «crime» est d'avoir alloué une infime

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

portion des ressources de leur ordinateur à des campagnes d'attaques par saturation organisées par d'autres.

Nous l'avons évoqué, les États-Unis se montrent particulièrement impitoyables dans le traitement judiciaire qu'ils réservent aux Anons et autres hacktivistes: non seulement les peines de prison y sont beaucoup plus longues qu'ailleurs, mais elles sont assorties d'amendes astronomiques. Des Anons américains tels que Jeremy Hammond et même des stratèges associés au collectif tels que Barrett Brown ont écopé de lourdes sentences après le hacking de Stratfor (nous reviendrons sur le cas du second). Lorsqu'ils auront été libérés, ces individus devront assumer l'écrasant fardeau financier des amendes qu'on leur a infligées.

Combinés à la découverte du fait que Sabu, un pilier d'Anonymous, a été informateur pour le Federal Bureau of Investigation (FBI) pendant des mois, ces châtiments ont alimenté la méfiance, la suspicion et la peur chez les Anons. Les équipes de hackers, qui supposaient depuis toujours que des taupes étaient planquées dans tous les recoins, sont devenues encore plus paranoïaques, réduisant leurs effectifs au strict minimum et renforçant la sécurité de leurs opérations. Elles ont aussi mis leurs fanfaronnades en sourdine.

En 2013, Anonymous semblait avoir essentiellement renoncé à s'infiltrer dans des systèmes informatiques. En fait, le collectif s'adonnait toujours à ce type d'activités, mais plus discrètement. C'est l'année où des Anons italiens ont en effet lancé de nouvelles campagnes de hacking et d'attaques par saturation, et où l'un des sous-groupes d'Anonymous les plus prolifiques, l'opération Green Rights (droits environnementaux), a hacké et défacé les sites de dizaines de sociétés peu scrupuleuses en matière d'environnement, dont Monsanto (pour une raison qui m'échappe, ces coups d'éclat n'ont jamais éveillé l'intérêt des médias ni débouché sur des enquêtes). En 2014 et en 2015, les campagnes les plus visibles d'Anonymous en Amérique du Nord et en Europe occidentale ont été axées plutôt sur la diffusion d'information et la sensibilisation que sur l'action directe. Au Royaume-Uni, l'opération Death Eaters (nécrophages) visait à attirer l'attention sur le problème de l'exploitation sexuelle des enfants et

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

sur la dissimulation des comportements pédophiles de personnages parmi les plus puissants du pays. Aux États-Unis, l'opération Ferguson avait pour but de soutenir et de faire connaître le mouvement de dénonciation de l'homicide d'un adolescent afro-américain non armé, Michael Brown, par un policier. L'opération ISIS, qui, à maints égards, reflète les intérêts des puissances occidentales, a pour objectif de déceler et de faire connaître les comptes Twitter et les sites web du groupe armé État islamique (EI) pour qu'on puisse les exclure du web.

Des opérations de hacking spectaculaires du genre de celles qui ont fait connaître Anonymous auprès du grand public continuent de faire la manchette, mais la plupart d'entre elles sont le fait de groupes de hackers n'ayant ni liens ni traits communs avec nos Anons assoiffés de justice sociale ou d'action politique. En fait, nombre d'entre eux défendent des positions diamétralement opposées à celles du collectif. En 2014, par exemple, Sony Pictures Entertainment a été la cible de mystérieux Guardians of Peace (gardiens de la paix), des hackers qui, prétendument en représailles à la sortie prochaine d'un long métrage parodiant le régime nord-coréen, ont divulgué une quantité impressionnante de données sensibles subtilisées à l'entreprise, dont des copies préliminaires de films à paraître, des procès-verbaux de réunions et des communications internes. Le sort s'est acharné une fois de plus sur Sony pendant les Fêtes de 2014, alors que Lizard Squad (un groupe semblable à LulzSec, mais dépourvu de plateforme politique déclarée) a fait passer de bons moments à ses abonnés Twitter en paralysant le réseau PlayStation le jour de Noël. En 2015, des hackers partisans de l'EI rassemblés sous le nom de «Cybercalifat» ont pris le contrôle d'un compte Twitter du gouvernement des États-Unis en janvier, d'un compte du magazine *Newsweek* en février, et de l'ensemble du système informatique de la chaîne de télévision francophone TV5 Monde en avril.

Mais les apparences sont parfois trompeuses. Le centre de gravité d'Anonymous s'est tout simplement déplacé vers des lieux moins visibles. En Amérique latine et dans certaines régions de l'Asie, des Anons, actifs depuis quelque temps pour la plupart, ont continué à se frayer un chemin

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

dans des systèmes informatiques. Une de leurs équipes les plus prolifiques, LulzSec Pérou, a mené des dizaines d'opérations: lors de l'une d'elles, elle a subtilisé des documents à l'armée de l'air chilienne et les a transmis au gouvernement du Venezuela. Une de ses opérations mémorables a eu lieu le 11 février 2014, alors qu'elle rendait publics des courriels prouvant la corruption du gouvernement péruvien. Comme l'a rapporté Frank Bajak, d'Associated Press (AP), la correspondance extraite du réseau du Conseil des ministres péruvien «a déclenché un tollé à l'échelle nationale» et «a étayé les accusations selon lesquelles des ministres de haut rang se comportaient davantage comme des lobbyistes que comme des serviteurs du bien commun. La fuite a contribué à l'adoption d'une motion de censure dont le cabinet est sorti très amoché[1]».

Bien que cette opération ait fait assez de bruit pour attirer l'attention de la presse anglophone, la plupart des grands médias occidentaux tendent à ignorer l'activité d'Anonymous ailleurs dans le monde. De toute évidence, même les journalistes disposés à couvrir ces événements sont généralement mal outillés pour le faire. En raison des barrières linguistiques et de la difficulté d'entrer en contact avec les hackers (plus réticents que jamais à parler depuis la vague d'arrestations), il est maintenant très difficile d'effectuer des reportages du genre de ceux qui se publiaient couramment à l'époque de LulzSec.

Le peu d'attention des médias à l'égard d'Anonymous témoigne sans doute moins d'un essoufflement du collectif que du fait qu'il a tout simplement aiguisé ses réflexes de survie. Grâce à leurs efforts de visibilité, AntiSec et LulzSec étaient certes devenus des forces que nul ne pouvait ignorer, mais, en définitive, leur présence publique était aussi leur plus grande faiblesse. Il est difficile de peser le pour et le contre des deux stratégies. C'est en se plaçant sous les feux de la rampe que LulzSec et AntiSec ont pu faire connaître leurs causes et attirer des recrues et des sympathisants; cependant, plus longtemps ces équipes stables agissaient sous le regard attentif des médias, du public et, en particulier, de l'État, plus leurs membres étaient susceptibles de se faire pincer. Chaque opération

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

qu'elles menaient – en particulier celles, fréquentes, dirigées contre les forces de l'ordre – augmentait leurs risques de se faire démasquer.

Néanmoins, comme c'est le cas de tout mouvement politique émergent dont le mode de fonctionnement et les stratégies n'ont jamais été mis à l'épreuve, les procédés souvent chaotiques d'Anonymous et son flirt avec la renommée ne pouvaient être qu'expérimentaux. Par conséquent, il n'est guère étonnant que ses résultats aient oscillé entre réussites éclatantes et échecs retentissants. Inévitables, les faux pas apportent leur lot de dommages collatéraux, mais les militants peuvent apprendre de leurs erreurs et de celles des autres.

Et il semble que certains observateurs aient été attentifs. Prenons l'exemple de l'opération de hacking de 2014 contre la société britannique Gamma Group, qui vend «des solutions techniques avancées de surveillance et de contrôle» aux États (dont des régimes dictatoriaux et répressifs qui utilisent ses outils contre des dissidents et des militants)[2]. En 2011, la firme a acquis une certaine notoriété lorsque WikiLeaks a publié une de ses vidéos de promotion ainsi que des brochures et des diaporamas où elle indiquait que ses logiciels peuvent servir à infecter un ordinateur[3]. Peu après, deux chercheurs en sécurité informatique ont évoqué la possibilité que le gouvernement du Bahreïn ait utilisé cette méthode pour installer subrepticement un logiciel appelé FinFisher sur les ordinateurs de militants par l'entremise de pièces jointes à des courriels. (Les représentants de Gamma ont réagi en affirmant que le logiciel leur avait été volé et qu'ils ne l'avaient donc jamais vendu au Bahreïn[4].)

Le 3 août 2014, un hacker disant s'appeler Phineas Fisher (Phineas est un nom grec signifiant «oracle») est arrivé sans crier gare en annonçant dans divers médias sociaux qu'il s'était introduit dans le système informatique de Gamma et venait de publier 40 gigaoctets de documents relatifs à FinFisher. Très variés, ceux-ci comprenaient des données techniques (plans de logiciels, codes sources, analyses de modes d'utilisation) ainsi que des listes de clients, des barèmes de prix, des tutoriels, etc. Fisher a aussi contribué à étayer la preuve de l'utilisation de FinFisher par le gouvernement du Bahreïn à l'encontre de militants[5]. Dans

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

une déclaration publiée avec la fuite, il encourageait ses camarades hackers à «riposter» et leur donnait quelques tuyaux. Ce «guide du bricoleur destiné à ceux qui n'ont pas la patience d'attendre les lanceurs d'alerte» commençait par le conseil suivant: «Tant que vous ferez preuve de bon sens en évitant toute activité liée au hacking ailleurs que sous Whonix, en ne révélant rien de votre vie réelle lorsque vous communiquez avec d'autres hackers, et en ne vous vantant jamais de vos exploits illicites auprès de vos amis du monde réel, vous pourrez faire pratiquement tout ce que vous voulez sans craindre de vous faire coffrer[6].»

Même si Phineas Fisher ne s'est pas présenté comme un sympathisant d'Anonymous, son opération de hacking en reflétait l'esprit, et il s'inspirait manifestement du style de divulgation introduit par LulzSec et d'autres sous-groupes du collectif. (Il a d'ailleurs montré qu'il était un fin connaisseur du *lulz* dans ce passage: «Ce n'est qu'après avoir échoué dans ma tentative de hacker tout le système de Gamma et avoir mis la main sur des documents intéressants, mais pas sur une copie du logiciel serveur FinSpy, que je me suis résigné à me contenter d'une solution de repli nettement moins imprégnée de l'esprit du *lulz*, à savoir de divulguer leurs documents en me moquant d'eux sur Twitter[7].») Par rapport à la multiplication des fuites et à l'essor de l'activité des lanceurs d'alerte (dont les plus illustres sont de braves citoyens comme Chelsea Manning et Edward Snowden) de ces dernières années, les méthodes de divulgation employées par Anonymous se distinguent par leur recours, risqué, à l'action directe: au lieu de mettre au jour des documents qu'on leur a transmis, les Anons s'insinuent eux-mêmes dans les réseaux des entreprises et des États en vue d'en extraire de l'information émanant des firmes de sécurité et de renseignement.

Phineas Fisher s'est cependant démarqué de ses semblables de LulzSec ou d'AntiSec, non par sa méthode ou le choix de sa cible, mais plutôt par une minutie, une précision et une prudence dont on n'a jamais vu Anonymous faire preuve. De plus, au lieu de profiter de cet instant sous les projecteurs pour faire son autopromotion, il a passé cinq jours à tenter

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

d'attirer l'attention sur les données qu'il avait publiées sur Twitter et Reddit, puis s'est évaporé dans la nature.

Le 5 juillet 2015, Phineas Fisher a refait surface en revendiquant la responsabilité d'une opération de hacking similaire, cette fois contre un fournisseur d'armes numériques encore plus honni, la société milanaise Hacking Team, qui qualifie ses logiciels de sécurité de «solutions offensives» et dont la clientèle variée va du FBI à l'armée de terre des États-Unis[8]. Fisher a pris le contrôle du compte Twitter de l'entreprise, dont il a changé le nom pour Hacked Team avant de lui faire publier cette annonce: «Parce que nous n'avons rien à cacher, nous rendons publics tous nos courriels, tous nos fichiers et tous nos codes sources [lien][9].» Avant d'être victime de l'opération, cette firme de mercenaires high-tech avait fait tout son possible pour dissimuler la véritable nature des services qu'elle offrait, ses transactions et sa clientèle. À l'instar de Gamma Group, Hacking Team prétendait n'avoir jamais vendu quoi que ce soit à des régimes répressifs. La divulgation d'une masse imposante de 400 gigaoctets de données a vite dissipé cet écran de fumée: elles indiquent que la firme n'a jamais hésité à faire affaire avec de tels régimes et s'est livrée à nombre d'autres pratiques douteuses, dont la rétention de vulnérabilités critiques touchant des logiciels, comme l'omniprésent Flash Player d'Adobe, lesquelles étaient potentiellement dangereuses pour des millions d'internautes.

Afin de prouver qu'il était bel et bien Phineas Fisher (et d'indiquer que d'autres opérations étaient à venir), le hacker a publié un tweet depuis le compte qu'il avait utilisé pour tourner Gamma Group en dérision (@GammaGroupPR): «Gamma et HT sont en panne. Quelques autres suivront», a-t-il écrit en ajoutant un nouveau lien vers son manifeste-guide du bidouilleur[10]. Les principes énoncés dans ce dernier n'ont rien de nouveau. Ils sont appliqués depuis belle lurette dans le milieu des hackers, y compris par l'élite d'Anonymous (dont beaucoup de membres, il importe de le préciser, ne se sont jamais fait arrêter et ne croupissent pas en prison). Néanmoins, parce qu'il est difficile de mettre en place des dispositifs de sécurité et que de nombreux Anons ont été épinglés, il est prudent de

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

rappeler les principes de base le plus souvent possible. Phineas Fisher implore ses recrues de ne pas lésiner avec la sécurité, tout comme le fait Anonymous depuis le «sabutage» de 2012. «Si vous êtes un néophyte, asseyez-vous, détendez-vous et observez», a tweeté Anon2earth. «Ne prenez part à aucune opération si vous ne savez pas ce que vous faites. Protégez-vous[11].» Au sein d'Anonymous, conseils et réprimandes en matière de sécurité font maintenant partie du quotidien.

Ces leçons semblent avoir été retenues non seulement par des hackers comme Phineas Fisher, mais aussi par de nombreux Anons. Prenons l'exemple de l'opération Cyber Privacy (vie privée en ligne), qui dénonce les nouvelles lois des pays occidentaux concernant la sécurité, telles que la proposition de loi C-51 adoptée en 2015 par le Canada et condamnée par des universitaires, des juristes, des journalistes et des dizaines d'associations de la société civile en raison des pouvoirs indus qu'elle accorde aux forces de l'ordre et aux agences de renseignement. Les Anons s'en sont d'abord pris au projet en misant sur la sensibilisation, mais, devant l'inefficacité de la stratégie et l'indifférence des médias, ils ont redonné vie à la bonne vieille tactique de l'attaque par saturation.

Le 17 juin 2015, Anonymous a paralysé des dizaines de sites web de l'État canadien, dont ceux du Service canadien du renseignement de sécurité (SCRS), du ministère de la Justice, du ministère de l'Industrie, du ministère des Affaires étrangères, du Commerce et du Développement, et du ministère des Ressources naturelles. Plus important encore, ils ont réussi à perturber les communications numériques du gouvernement en s'en prenant délibérément à un serveur de courriel. La campagne a été largement couverte par les médias. Selon le *Globe and Mail*, «il s'agit de la cyberattaque la plus spectaculaire qu'ait connue le Canada depuis que des hackers chinois se sont introduits dans le système de son principal centre de recherche scientifique l'an dernier[12]». Peu de temps après l'opération, un de ses organisateurs m'a expliqué que «les principaux membres de l'équipe de travail» avaient étroitement collaboré «pendant sept mois» sur diverses opérations, allant «de la traque des policiers de Ferguson à la défense de la vie privée, en passant par la révolution ukrainienne, la dénonciation du Ku

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Klux Klan et la chasse aux pédophiles». Certains de ces Anons étaient des nouveaux venus, mais le groupe de base était surtout constitué de vétérans. Soulignant le fort contraste avec l'opération Avenge Assange de décembre 2010 contre PayPal, qui avait conduit à l'arrestation de nombreux participants, mon interlocuteur a affirmé que la sécurité était devenue une telle priorité qu'un de leurs objectifs consistait désormais à éviter tout dommage collatéral, c'est-à-dire toute négligence qui pourrait amener les autorités à intensifier leur répression. Le hacker a conclu notre échange en notant avec fierté que son équipe n'avait encore connu aucun «raté [en matière de sécurité]. Ce qui est très bien». Quelque temps après, il m'a indiqué que nous avions déjà chatté par le passé, mais qu'il utilisait alors un pseudo différent. Désormais, a-t-il ajouté, les noms sont traités comme des téléphones jetables qu'on remplace périodiquement: quand un militant réapparaît, il est considéré comme un Anon différent, ce qui le rend plus difficile à associer à une opération antérieure.

De telles mesures de prudence auraient été difficilement imaginables si les arrestations de 2011 et de 2012 n'avaient pas eu lieu – mais leur efficacité reste à démontrer. Il semble que beaucoup d'Anons ne savent toujours pas très bien comment ils pourront s'en tirer – et ce qu'ils risquent précisément. Une bonne partie de l'évaluation dépend du traitement et des conséquences judiciaires que subiront les personnes arrêtées.

Des 14 personnes arrêtées dans le cadre de l'attaque contre PayPal, 13 ont été accusées de crime grave et de délit mineur (les accusations de crime grave seraient finalement retirées à la suite d'une négociation de peine); 11 d'entre elles ont plaidé coupable, et 2 ont été condamnées à trois et quatre ans de résidence surveillée respectivement, ce qui leur a permis d'éviter une sentence pour crime grave. Les 13 ont été condamnées à verser 5 600 dollars en dédommagement à PayPal et à eBay (alors société mère de PayPal); celles qui n'avaient pas les moyens de s'acquitter de la somme en un seul versement se sont vues contraintes d'effectuer des paiements mensuels de 100 dollars. Le 14^{e} membre du groupe, Dennis Owen Collins, était un des participants les plus dévoués d'AnonOps (il apparaît dans ce livre sous les pseudos de Fred et d'Owen). Le 16 juillet 2015, après avoir

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

passé un peu moins d'un an en détention à domicile, il est mort à l'âge de 54 ans des suites d'une maladie pulmonaire chronique et débilitante dont il aura souffert pendant presque toute sa vie adulte.

De toutes les causes impliquant Anonymous qu'ont entendues les tribunaux américains, celle de Barrett Brown se situe dans une classe à part. Le 22 janvier 2015, dans une salle d'audience pleine à craquer, le juge Samuel Lindsay a prononcé une sentence sévère à l'encontre du journaliste et agitateur. Brown, qui avait alors déjà passé plus de deux ans derrière les barreaux, a été condamné à trente-cinq mois supplémentaires de prison et à des dommages et intérêts de près d'un million de dollars à verser à la firme de sécurité informatique Stratfor. Il avait initialement fait face à 17 chefs d'accusation, mais sa sentence potentielle avait été réduite à un maximum de huit ans grâce à une négociation de peine. Il n'a finalement été condamné que pour trois crimes: menaces contre un policier fédéral, obstruction à un mandat de perquisition et complicité après le fait avec les hackers d'Anonymous qui s'étaient infiltrés dans le système informatique de l'entreprise d'Austin pour le vider de son contenu.

L'élément le plus insolite (et le plus discutable) de ce procès est l'affirmation du juge selon laquelle Brown n'a «pas simplement rapporté les activités des hackers», mais a plutôt contribué à leur organisation: «Le tribunal conclut que M. Brown a collaboré avec les hackers et les a soutenus, a localisé des cibles, a donné des conseils, a élaboré des stratégies et a participé à l'organisation d'activités de hacking[13].»

Pourtant, le fait est que Brown n'était pas un hacker; de plus, on ne l'a jamais accusé officiellement du moindre crime de hacking. Dans Anonymous, il jouait avec passion le rôle de stratège. On n'a pas prouvé qu'il avait coordonné l'infiltration de décembre 2011 dans les systèmes de Stratfor ou qu'il y avait participé. Bien qu'il ait partagé un lien vers les numéros de carte de crédit volés par les Anons, il s'intéressait avant tout aux courriels. Cela lui a d'ailleurs valu un chef d'accusation, le plus controversé des 17 auxquels il a d'abord fait face: il n'avait ni volé ni utilisé les données des cartes, et avait simplement fait suivre un lien qui circulait déjà. En mars 2014, l'accusation a été retirée, mais le juge s'est néanmoins

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

rangé aux arguments des procureurs, selon lesquels la publication d'un lien vers les données volées avait aidé les hackers et devait donc être considérée comme pertinente pour la détermination de la sentence. «Il ne s'agissait pas d'un simple partage de lien, mais d'un geste qui s'inscrivait dans sa collaboration avec les autres participants à une même activité», a-t-il conclu[14]. Par conséquent, malgré le retrait de l'accusation, Brown s'est vu infliger une peine plus longue.

Ce type de contorsion judiciaire ne peut que nuire à la liberté d'expression, car cela crée une situation où d'autres journalistes seront moins enclins à partager des liens, craignant que le geste puisse être interprété comme une circonstance aggravante par un tribunal (dans la foulée du prononcé de la sentence, la journaliste Quinn Norton a d'ailleurs annoncé qu'elle cessait de couvrir les fuites, la sécurité informatique et les hackers par crainte de représailles similaires[15]). Comme bon nombre de hackers, de lanceurs d'alerte, de journalistes et de militants qui ont tout risqué pour défendre la liberté de la presse et l'obligation de rendre des comptes, Brown en paie le prix fort. Sa sentence témoigne d'une volonté de l'État de poursuivre non seulement les hackers politisés, mais aussi les geeks et les journalistes qui, à l'instar de Brown, collaborent étroitement avec eux.

Le traitement judiciaire impitoyable des hackers militants américains et de leurs sympathisants est au cœur d'une affaire qui fait rage au moment où j'écris ces lignes. Le 15 juillet 2015, le hacker britannique Lauri Love a été arrêté dans son pays; il risque d'être extradé vers les États-Unis, où il est mis en accusation en vertu de la Computer Fraud and Abuse Act (CFAA) pour de présumées opérations de hacking contre la NASA, l'armée de terre des États-Unis et la Réserve fédérale américaine dans le cadre de l'opération Last Resort, consécutive au suicide du hacker Aaron Swartz. Les sympathisants de Love font tout pour empêcher son extradition: si on l'envoie aux États-Unis pour être jugé, craignent-ils, il risque une punition beaucoup plus sévère, ce qui pourrait l'amener à choisir le même sort tragique que Swartz. «L'extradition de Lauri Love aux États-Unis constituerait une grave violation de ses droits», écrivent-ils[16].

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

L’État a toujours compté sur ses pouvoirs de poursuite et de répression pour mettre en place un climat de peur capable d’écraser les mouvements politiques, ou à tout le moins de freiner leur croissance. C’est pourquoi il est remarquable que tant de geeks et de hackers, loin de se laisser dissuader par la réaction des autorités, aient été poussés à agir avec une ardeur renouvelée. Les révélations d’Edward Snowden, en particulier, ont été perçues comme un signal d’alarme historique: elles ont galvanisé bien des gens et donné une vigueur nouvelle aux mouvements pour la protection de la vie privée, qui se sont lancés dans le développement d’outils de cryptage.

Depuis leur arrestation, de nombreux ex-membres d’Anonymous, de LulzSec et d’AntiSec ont continué à participer activement au mouvement pour la protection de la vie privée. À l’été 2015, Donncha O’Cearbhaill a été sélectionné pour effectuer un stage d’été dans les rangs de l’organisme chargé du réseau de routage anonyme Tor sous la supervision d’un de ses principaux développeurs. Lors de son entretien d’embauche, on lui a posé la question suivante: «Qui sont vos héros, si vous en avez, en matière de liberté d’internet?» Le jeune homme a répondu par un éloge de ses collègues et de l’ensemble de la communauté des hackers: «Nombreux sont les membres du mouvement pour un internet libre qui m’inspirent. Je suis particulièrement reconnaissant à des gens comme Edward Snowden, Julian Assange et Jeremy Hammond, qui ont fait des sacrifices considérables pour tenter de faire la lumière sur la surveillance exercée par l’État, de plus en plus généralisée. Les développeurs et les défenseurs du logiciel libre de partout m’inspirent également[17].» Quant à Mustafa Al-Bassam, toujours stagiaire à Privacy International, il a diversifié ses contributions. Lorsque les données de Hacking Team ont été divulguées, il s’est empressé d’en héberger une copie sur un site personnel afin qu’on puisse les télécharger à tout moment. Celles-ci sont très recherchées; pendant des jours, le site a reçu tellement de visites que le hacker a dû travailler jour et nuit pour le maintenir en service. Al-Bassam collabore aussi avec des chercheurs en sécurité informatique et d’autres anciens Anons, dont Darren Martyn, au sein d’un groupe de réflexion officieux appelé LizardHQ. Jusqu’ici, ils ont attiré l’attention sur les vulnérabilités d’outils de surveillance douteux

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

comme Hola (réseau privé virtuel [VPN] pourvu d'une porte dérobée par laquelle les ordinateurs de ses dix millions d'utilisateurs peuvent être recrutés dans des *botnets*), E-Detective (dispositif légal d'interception employé notamment par les forces armées chinoises et plus de 100 corps policiers dans le monde) et Impero (logiciel espion à l'aide duquel certaines écoles du Royaume-Uni surveillent leurs élèves). Al-Bassam m'a expliqué que LizardHQ avait pour objectif d'en «révéler les vulnérabilités afin que les gens puissent prendre des décisions éclairées relativement aux systèmes qu'ils utilisent et qui font peu de cas de leurs libertés civiles. [...] Nous ne coordonnons pas nos divulgations de vulnérabilités avec les firmes qui vendent des logiciels espions ni ne les en informons au préalable, car une telle collaboration entre chercheurs en sécurité informatique et développeurs de logiciels espions établirait un dangereux précédent».

De nombreux sondages confirment que, depuis Snowden, le grand public américain se préoccupe davantage qu'auparavant des enjeux liés à la protection de la vie privée[18]. Les Nations Unies sont aussi intervenues dans le dossier: leur Haut-Commissariat aux droits de l'homme a publié un rapport qui défend la nécessité démocratique «du chiffrement et de l'anonymat dans les communications numériques», lesquels «permettent aux individus d'exercer leurs droits à la liberté d'opinion et d'expression à l'ère numérique et méritent de ce fait d'être fortement protégés[19]».

Cependant, malgré l'évolution de l'opinion publique, les forces policières et d'autres représentants des autorités réagissent de façon prévisible (comme elles le font depuis des décennies), en diabolisant autant les technologies de cryptage que l'idéal d'anonymat sur lequel elles reposent. Face aux pressions des utilisateurs, des développeurs de logiciels propriétaires comme Apple et Google ont fait des efforts considérables pour améliorer la sécurité de leurs produits, suscitant la réprobation du FBI et d'autres agences chargées de l'application de la loi, pour qui ces entreprises se doivent plutôt d'«empêcher le cryptage avant toute chose». En octobre 2014, à la Brookings Institution de Washington, le directeur du FBI a tenu un discours alarmiste et virulent sur la vie privée: «Avec tous ces gens qui entrent dans l'ombre, nous, qui sommes chargés du maintien de l'ordre et

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

de la sécurité publique, craignons fortement de laisser passer des prédateurs qui exploitent des personnes vulnérables, des criminels violents qui veulent s'en prendre à nos collectivités, et des cellules terroristes qui utilisent les médias sociaux pour recruter, planifier et lancer une attaque[20].»

Bref, une bataille rangée sur l'avenir de la vie privée et de l'anonymat fait rage. Le conflit n'a certes rien de nouveau, mais ce n'est que récemment qu'il a cessé d'être cantonné aux cénacles des théoriciens du droit, des responsables politiques, des technologues et des universitaires, et que des collectifs de technologie, des avocats, des journalistes, des cinéastes, des hackers, des développeurs de logiciels ou de matériel informatique, des ONG et des citoyens inquiets sont entrés dans la mêlée. À l'instar de l'idéal de la liberté d'expression, qui a pénétré la conscience collective lors de combats politiques épiques (comme les luttes ouvrières du syndicat Industrial Workers of the World [IWW] à Spokane au début du xx^{e} siècle ou les rassemblements pour la liberté d'expression à Berkeley dans les années 1960), les initiatives citoyennes pour la protection de la vie privée semblent s'approcher de la masse critique.

La place qu'occupe Anonymous dans ce tout nouveau mouvement citoyen pour la protection de la vie privée mérite qu'on s'y attarde. Évidemment, vu son nom et sa symbolique, le collectif témoigne, par son existence même, de son attachement aux valeurs en cause. Toutefois, cette grande proximité avec un mouvement social représente à bien des égards une arme à double tranchant: bien qu'Anonymous puisse populariser des enjeux et attirer des sympathisants, il peut aussi alimenter la critique de ses détracteurs. Compte tenu du penchant des Anons pour la controverse, il faut d'ailleurs s'y attendre. Il est impossible de calmer une polémique qu'ils alimentent, et, même lorsque celle-ci constitue leur intention première, les résultats peuvent être imprévisibles et improductifs, voire nuisibles.

Néanmoins, plus que tout autre mouvement politique d'hier ou d'aujourd'hui, Anonymous représente un cas d'espèce pour qui souhaite réfléchir au fonctionnement, aux avantages, aux contradictions et aux limites de l'anonymat en action. Alors que le mouvement pour la protection de la vie privée prend forme, je constate qu'il y a une tension

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

caractéristique chez les gens qui considèrent l'anonymat comme un instrument utile sur le plan politique. Bien qu'ils appuient sans réserve l'idée d'un droit au cryptage, nombreux sont les progressistes et les libéraux qui éprouvent un profond malaise à l'égard du recours au secret par des militants, du rôle de l'anonymat en général et de la fonction d'Anonymous en particulier. Autrement dit, ils déplorent le fait que les Anons (et les militants anonymes en général) ne rendent pas de comptes, et que, d'un certain point de vue, ils fassent preuve de lâcheté. Dernièrement, un universitaire a exprimé ce malaise sans mâcher ses mots: «Le contraire de l'anonymat, c'est la responsabilité.»

Le lien entre anonymat et irresponsabilité est certes beaucoup plus complexe que ce que laisse entendre cette assertion, mais il faut admettre qu'une des caractéristiques fondamentales de l'incognito volontaire réside dans la possibilité d'échapper au fardeau de la responsabilité. C'est sur cette base même que la philosophe Helen Nissenbaum, spécialiste des questions relatives à la vie privée, se porte à la défense de l'anonymat: «La valeur de l'anonymat ne réside pas dans la possibilité de ne pas être nommé, mais plutôt dans celle d'agir ou de participer en restant hors d'atteinte», écrit-elle[21].

Bien qu'un minimum de secret offre une certaine protection contre de possibles conséquences judiciaires et constitue donc un outil essentiel à Anonymous, les arrestations de membres de LulzSec et d'autres participants rappellent aux Anons d'aujourd'hui que l'anonymat n'est jamais absolu, qu'il est toujours relatif à la position de l'observateur. De nombreux Anons sont conscients des risques qu'ils courent et agissent en conséquence, organisant leurs opérations en faisant comme s'ils allaient être démasqués à coup sûr (même s'ils espèrent ne pas l'être). Il leur arrive aussi de rejeter cet anonymat rigide, technique, motivé par la sécurité, et de s'en tenir à l'anonymat social, grâce auquel ils peuvent interagir avec leurs pairs sur une base égalitaire. Un des 14 Anons arrêtés dans la foulée des opérations Payback et Avenge Assange, Keith Wilson Downey, l'a admis en revenant sur sa participation: «Je défendais la liberté d'expression depuis plus de dix ans, et j'ai décidé que je n'allais plus me contenter de parler. Le

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

9 décembre 2010, j'ai téléchargé LOIC [Low Orbit Ion Cannon], je me suis connecté à la ruche et j'ai pris part à la protestation contre PayPal. Il importe de noter que j'ai aussi choisi de ne pas effacer mes traces, car je considérais que cette campagne était légitime et valait le risque. Cette décision aura changé ma vie pour trois ans[22].» Pour Downey, l'anonymat n'était pas une carapace contre la responsabilité, mais un cadre à partir duquel agir.

Il est difficile de réduire la mécanique de l'anonymat propre à Anonymous à une logique simple: peu importe comment on résume celui-ci, quiconque le désire peut l'adopter et lui attribuer de nouveaux usages, de nouveaux protocoles, de nouvelles fins. Personne ne peut posséder l'anonymat, et encore moins le contrôler, car toute tentative en ce sens change sa nature même; il s'agit en quelque sorte d'un idéal incorruptible (ou infiniment corruptible), toujours inaccessible au pouvoir, même si les gens qui en font (ou croient en faire) l'expérience peuvent se faire attraper. Quoi qu'il en soit, Anonymous a incontestablement rendu possible l'avènement d'une nouvelle position pour le sujet politique, une position d'où l'on ne se «contente plus de parler», pour reprendre la formule de Downey, et où seule l'*action* compte; où une action peut être évaluée, mais où tous les participants considèrent leur identité comme moins importante que leurs gestes, même s'ils risquent d'être identifiés et emprisonnés. De cette façon, même s'ils sont nommés, la valeur de l'anonymat dont ils ont cru bénéficier est maintenue dans les actions que celui-ci leur a permis d'accomplir. La foi dans l'idée d'Anonymous suffit à motiver l'action, même si l'anonymat total n'est pas l'objectif poursuivi ou reste inaccessible.

Il importe également de souligner que, même si les Anons se cachent derrière un pseudonyme lorsqu'ils agissent ouvertement, leurs opérations comme telles n'ont absolument rien de secret. Ces militants s'organisent sur des canaux Internet Relay Chat (IRC) publics, diffusent des communiqués de presse et exposent leurs arguments dans des vidéos pittoresques. De plus, ils entretiennent généralement des contacts directs avec des militants locaux qui ne font pas partie d'Anonymous, de même qu'avec des journalistes.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Dans les premiers jours de l'opération Ferguson, par exemple, CNN était en communication avec des participants aux canaux IRC dans le but de les amener à donner des interviews en direct à la télévision. On imagine difficilement qu'un journaliste puisse avoir un tel accès à des terroristes ou à des hackers criminels, qui font tout pour éviter le moindre contact avec l'État et le grand public. En d'autres termes, la plupart des Anons ne se cachent pas dans l'équivalent numérique des cavernes de Tora Bora en vue de comploter à l'abri des regards. Ils agissent essentiellement au grand jour – mais en veillant juste assez à leur sécurité pour être en mesure d'agir.

Qui plus est, il est d'ordinaire assez facile d'attribuer une opération à un groupe, à un compte Twitter, à un réseau IRC ou à un individu en particulier. À titre d'exemple, prenons l'opération Cyber Privacy. Peu après que le groupe qui l'a lancée eut mené une série d'attaques par saturation pour dénoncer le projet de loi C-51, un autre hacker d'Anonymous, connu sous le pseudo de ro0ted, a annoncé qu'il venait de hacker un site web du gouvernement canadien et avait rendu publics les noms et les références de fonctionnaires. La presse a d'abord attribué l'action aux Anons de l'opération Cyber Privacy. Mais ces derniers, qui n'y avaient joué aucun rôle – et qui la critiquaient vertement en la qualifiant de violation irresponsable de la vie privée –, se sont empressés de contacter les journalistes pour leur demander de publier un rectificatif. Quiconque aurait fait un minimum de recherche aurait constaté que ro0ted se réclamait bel et bien d'Anonymous, mais pas de l'opération Cyber Privacy: il était plutôt membre du réseau de cyberguérilla du collectif[23]. La plupart des articles ont été vite corrigés, avec une précision sur une caractéristique d'Anonymous: même les gens qui agissent sous le couvert d'un minimum d'anonymat savent assumer leurs responsabilités[24].

Même si la plupart des actions menées au nom d'Anonymous peuvent être associées à une entité qui prend soin de répondre aux questions qu'on lui pose, de nombreux observateurs persistent à se préoccuper de l'enjeu de la responsabilité lorsque cette dernière ne peut être attribuée à une identité juridiquement définie. On m'a souvent posé la question suivante: si Anonymous est clandestin, comment ses membres peuvent-ils assumer la

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

responsabilité de leurs actes devant les collectivités auprès desquelles ils travaillent?

Il vaut cependant la peine de se demander à quel point une telle responsabilité est possible dans des collectivités qui affirment être transparentes et rendre des comptes. Pour examiner la question d'un peu plus près, citons le cas du journalisme, souvent présenté comme l'exemple même de la transparence. Les journalistes publient des articles signés de leur vrai nom, et la crédibilité des médias repose sur la publication de faits et non de mensonges. Pourtant, on accepte la nécessité – souvent présentée comme un droit inaliénable – pour les journalistes de s'appuyer au besoin sur des sources anonymes, en particulier si l'information recherchée ne peut être obtenue autrement.

Il arrive cependant à des journalistes de se livrer à une pratique similaire à l'une de celles qu'on reproche à Anonymous: le *doxing*, c'est-à-dire la divulgation des noms d'individus jugés louches, qui se retrouvent alors en situation délicate. Il s'agit là, on le comprend, d'une des tactiques du collectif les plus controversées, qui prend parfois un tour ignoble. Comme nous l'avons vu dans ces pages, le *doxing* suscite souvent des grincements de dents chez certains Anons, en particulier lorsque ses victimes sont innocentes. Cela s'est produit dans le cadre de l'opération Ferguson lorsque le nom et des photos d'un policier qu'on croyait à tort responsable de l'homicide de Michael Brown ont été publiés sur le compte Twitter @TheAnonMessage.

Bien que les journalistes ne soient jamais accusés de *doxing* comme tel, leurs gestes ont parfois les mêmes conséquences. Et celui-ci n'est pas pratiqué uniquement par des tabloïds ou des sites comme *Gawker*, dont le fondateur a commis cette célèbre fanfaronnade: «J'applique un examen de passage éditorial tout simple: est-ce que c'est vrai? est-ce que c'est intéressant[25]?» Le *doxing* le plus notable de l'année 2014 n'est pas celui qu'Anonymous a fait subir par erreur au policier de Ferguson, mais un dossier du magazine *Newsweek*.

En mars 2014, *Newsweek* relançait son édition papier en grande pompe en publiant un article fracassant, annoncé en couverture: ses journalistes

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

prétendaient avoir établi la véritable identité de Satoshi Nakamoto, célèbre créateur pseudonyme de la cryptomonnaie Bitcoin. Ce nom d'emprunt, affirmaient-ils, n'était pas entièrement faux, car le personnage insaisissable qui aurait été le cerveau de la populaire devise numérique se serait appelé Dorian Nakamoto, un Nippo-Américain d'âge mûr établi dans le sud de la Californie. L'enquête, l'article et leurs suites, qui respectaient la forme et la logique d'un *doxing* mis en œuvre par des hackers, relevaient carrément de l'intrusion. La journaliste Leah McGrath Goodman a publié une photo de la maison de Nakamoto dont l'adresse était parfaitement lisible, tout comme le numéro de plaque d'immatriculation d'une voiture. La traque qui a suivi s'est ainsi avérée enfantine. L'information, communiquée à des millions d'Américains, était assortie d'une foule de détails sur la vie privée du monsieur, allant de ses finances personnelles à son état de santé, en passant par ses déboires conjugaux. Par la suite, le *Los Angeles Times* et une dizaine d'autres médias se sont lancés dans une «chasse au Bitcoin», lors de laquelle leurs reporters accompagnés de photographes ont piégé Nakamoto chez lui, allant jusqu'à le poursuivre dans un ascenseur pour l'interroger. Dans leurs articles, ils se moqueraient de lui parce qu'il a fini par sortir de la maison pour affronter la meute de journalistes en offrant à l'un d'eux une interview en échange d'un repas.

Un nombre incalculable d'experts, de journalistes et de commentateurs ont reproché à *Newsweek* la légèreté des preuves brandies pour corroborer l'identification. Néanmoins, malgré cette condamnation quasi unanime, le magazine a persisté, de façon peu convaincante, à défendre le reportage en invoquant l'intérêt public: «Nous avons jugé qu'il était dans l'intérêt du public d'établir certains faits essentiels relatifs à Bitcoin et de bien informer les personnes susceptibles d'y investir des fonds[26].» Et même si les journalistes avaient identifié la bonne personne, les considérations éthiques au nom desquelles ils ont jeté sa vie privée en pâture au public resteraient douteuses. À maintes reprises, le fondateur de Bitcoin a exprimé son désir de garder l'anonymat. Plus important encore, ses actes n'ont porté préjudice à personne, et, contrairement à ce que laisse entendre la direction de

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Newsweek, rien ne sert d'être au courant des détails de sa vie privée pour faire des «investissements judicieux» dans Bitcoin.

Bien sûr, parce qu'il est une entité juridique de droit public, le magazine peut faire l'objet de poursuites judiciaires – une option que Nakamoto aurait d'ailleurs envisagée. En revanche, il est pratiquement impossible de poursuivre un collectif sans visage pour cause de *doxing*, à moins que le responsable ait été préalablement arrêté par les autorités ou dénoncé par ses pairs. En raison des torts que *Newsweek* lui a causés, Nakamoto pourrait toucher une grosse somme d'argent[27], alors que l'indemnité obtenue par le policier doxé par erreur s'est limitée à des menaces de mort et à l'impossibilité d'être dédommagé.

La juxtaposition de ces deux cas fait ressortir des différences importantes entre la responsabilité d'une entité contestataire dissimulée comme Anonymous et celle d'une personne ou d'une institution connue. Mais d'autres inexactitudes ou omissions de la presse ont fait des dégâts beaucoup plus graves que tout ce dont Anonymous serait normalement capable de faire. Alors qu'un *doxing* fautif du collectif peut nuire dangereusement à une poignée d'individus tout au plus, une erreur bêtement répétée par les grands médias peut orienter des décisions qui auront un impact sur le sort de pays entiers. Ce qui constitue encore à ce jour le mensonge journalistique le plus grossier et le plus insidieux du XXIe siècle est si impressionant qu'il est presque inutile de le mentionner: celui-ci s'est répandu lorsque, tel un perroquet, le *New York Times* a répété la position du gouvernement des États-Unis selon laquelle Saddam Hussein accumulait des armes de destruction massive. Comme l'ont souligné de nombreux observateurs, cet article à lui seul a contribué à la justification d'une guerre atroce et extrêmement coûteuse en Irak, une décision politique à laquelle aucune poursuite judiciaire ni réaction citoyenne ne pourra jamais remédier.

Bien qu'on puisse considérer cet épisode comme une exception à cause de son caractère extrême, les exemples plus banals d'impairs journalistiques néfastes fondés sur des affirmations gratuites, eux, ne manquent pas, et se rapportent souvent à du militantisme en lien avec les nouvelles technologies. De nombreux journaux britanniques ont, par

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

exemple, publié des reportages qui vilipendaient Edward Snowden en le qualifiant d'espion russe sans même avoir tenté d'en fournir la preuve. Julian Assange, qu'on a si souvent taxé d'irresponsable pour les fuites qu'il facilitait, a étrillé un journaliste du quotidien *The Guardian* qui avait divulgué un mot de passe interne en l'utilisant comme titre d'un chapitre d'un livre où il relatait sa collaboration avec WikiLeaks. Selon Assange, cette imprudence a conduit à la «diffusion sur internet de centaines de câbles diplomatiques non caviardés du département d'État[28]». Il avait confié le mot de passe à quelques journalistes triés sur le volet en leur indiquant expressément que le matériel devrait être soigneusement validé avant publication pour éviter que des innocents soient doxés par inadvertance.

Penchons-nous enfin sur un cas directement lié à Anonymous, dont nous avons fait état dans l'avant-propos. En février 2012, alors que le collectif était au sommet de sa popularité (et que les parlementaires polonais revêtaient le masque de Guy Fawkes pour dénoncer un accord commercial), la journaliste du *Wall Street Journal* Siobhan Gorman a publié un article où l'on présentait les hackers militants comme de dangereux extrémistes. Selon le général Keith Alexander, alors directeur de la National Security Agency (NSA), Anonymous aurait «la capacité, d'ici un an ou deux, de provoquer une panne de courant limitée en menant une cyberattaque», pouvait-on y lire. La preuve était si mince que c'en était embarrassant; elle se réduisait à une seule phrase: «Le général Keith Alexander [...] a communiqué cette évaluation lors de réunions à la Maison-Blanche et d'autres rencontres privées, ont affirmé des habitués[29].» Non seulement l'affirmation était douteuse, mais elle ne concordait guère avec les pratiques connues d'Anonymous, si bien que l'article tombait à plat. S'il en avait été autrement, il aurait pu réduire à néant les efforts de tout un mouvement politique en vue de soutenir diverses causes sociales.

Anonymous fait parfois des erreurs, comme la presse. Toutefois, quand une faute est commise par un quotidien réputé, on ne réagit pas en condamnant l'ensemble du journal, voire du secteur journalistique, mais plutôt en critiquant l'article en cause, son auteur ou le rédacteur en chef de

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

la publication. Pourquoi devrait-il en être autrement pour Anonymous? Qu'elle soit le fait d'Anonymous, du *New York Times* ou de *Newsweek*, toute erreur mérite d'être vivement critiquée. C'est précisément ce qui s'est produit pendant l'opération Ferguson, lorsque le participant TheAnonMessage a publié un nom erroné. J'étais justement connectée au canal IRC juste avant que ça ne se produise. C'était tôt le matin, et la plupart des membres de l'opération n'étaient pas en ligne ou étaient inactifs. D'habitude, les opérations de *doxing* se déroulent derrière des portes closes, sur des canaux privés; mais curieusement, dans ce cas, TheAnonMessage n'a pas consulté l'équipe de base et a agi au grand jour. Une fois le nom rendu public (une erreur flagrante), presque tous les membres de l'opération, furieux, lui sont tombés dessus. Les reproches les plus acerbes lui sont venus de Crypt0nymous, vidéaste respecté du collectif. Dans une diatribe forte de dizaines de messages Twitter, celui-ci a dénoncé un geste bâclé et irresponsable, motivé à ses yeux par la soif de célébrité[30]. De telles volées de bois vert spontanées ne suffisent sans doute pas à redresser tous les torts, mais elles ont néanmoins un effet concret, généralement positif, sur les activités ultérieures du groupe.

En citant quelques exemples journalistiques, je ne cherche pas à justifier les opérations de *doxing* menées par Anonymous et leurs conséquences néfastes. Le péché des uns n'absout pas celui des autres. Je souhaite simplement rappeler que la transparence, à elle seule, ne constitue pas une garantie de prise de responsabilités. Quand des journaux renommés comme *The New York Times* ou *The Wall Street Journal* diffusent de fausses infos ou des articles fondés sur du vent, les conséquences peuvent être beaucoup plus dévastatrices que si la publication émane d'une organisation comme Anonymous. Car ces grands quotidiens sont perçus comme des sources d'objectivité, de vérité, et leur réputation est difficilement ébranlable. Les affirmations d'Anonymous, en revanche, sont souvent accueillies avec un certain scepticisme, y compris par des sympathisants.

On peut d'ailleurs féliciter Anonymous de ne pas dissimuler ses partis pris, inhérents à tout milieu producteur d'information – que ceux-ci soient attribuables à une limitation réelle des connaissances, à une surcharge

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

d'informations, à des préjugés, à des données erronées ou à de la pure et simple manipulation. Le fait de savoir que le collectif est faillible a une valeur en soi. Les Anons ne prétendent pas être objectifs, justes et équilibrés. Ils se considèrent simplement comme des activistes qui font de leur mieux (ou qui font de leur mieux pour être *malicieux*). Par conséquent, leurs erreurs ne peuvent s'avérer trop dommageables: personne ne s'attend à ce qu'ils soient irréprochables en tout temps, un privilège dont ne jouit pas une institution de renom comme *The New York Times.*

Mais la comparaison entre Anonymous et les médias d'information s'arrête là. Le champ d'activités du collectif, qui, rappelons-le, est un mouvement politique tourné vers l'action, est beaucoup plus vaste que celui de la presse, dont le mandat se limite à la diffusion de l'information. Bien que, dans de nombreux cas, le groupe responsable d'une opération d'Anonymous ait des comptes à rendre en interne, les actions directes les plus radicales du collectif requièrent parfois le secret et l'anonymat absolus, même entre Anons. Les plus risquées d'entre elles, en particulier, sont souvent mises en œuvre dans des recoins secrets par des «factions à même d'autres factions», comme nous l'avons vu précédemment. Les Anons n'ont d'ailleurs pas recours au secret uniquement pour assurer leur sécurité, mais aussi pour maintenir une certaine harmonie dans leurs rangs. S'ils ostracisent ceux qui font montre de vantardise, ce n'est pas simplement pour des raisons de sécurité personnelle, mais aussi pour réfréner l'égocentrisme.

Cette double fonction de la discrétion illustre ce que le professeur de communication Jack Bratich qualifie de «secret populaire mineur», dont la valeur consiste à «offrir une contrepartie à une sphère politique fondée sur l'identité et la représentation[31]». Souvent, explique-t-il, les efforts déployés par les mouvements sociaux pour gagner en visibilité et être mieux représentés ont moins pour effet de faire aboutir leurs revendications politiques que de les rendre plus vulnérables aux mécanismes de cooptation ou de rejet de l'État[32]. Ce dernier «a en aversion tout masque qui n'est pas le sien», note Bratich. Ainsi, sa propension à «diaboliser» les masques portés par ses citoyens tout en refusant obstinément d'enlever le sien

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

témoigne d'un important déséquilibre dans le rapport de force. Par conséquent, soutient le professeur, les militants auraient intérêt à réserver une place importante (quoique limitée) au secret, au risque sinon de renforcer le pouvoir de l'État sans le savoir: leur transparence révèle leurs vulnérabilités, dont un adversaire masqué peut tirer parti en toute sécurité.

Qu'ont à gagner les militants en adoptant des formes limitées de dissimulation, en particulier si celles-ci sont renforcées par une éthique de la discrétion visant à promouvoir l'égalitarisme? Aussi, peut-on justifier le recours au secret du point de vue de l'éthique s'il est le fait de groupes opprimés, tout en le condamnant sans appel s'il est le fait d'entités avantagées ou détentrices du pouvoir, tels que l'État et les acteurs économiques de premier plan? Lorsqu'il sert non seulement d'outil, mais aussi de mode de fonctionnement général (et en perpétuelle expansion) aux États-nations (comme on le voit, en particulier, chez les agences de renseignement, pourvues de moyens techniques et financiers en apparence illimités), le secret peut aller à l'encontre de l'intérêt public[33]. En revanche, aux militants ayant peu de ressources comme les Anons, il offre la possibilité de riposter contre les puissants. Il égalise les chances. Appliqué de façon limitée, le secret peut transformer le paysage politique pour le mieux en créant des conditions structurelles permettant d'agir (et non seulement de débattre et de communiquer) au nom de principes, et peut aussi constituer une forme d'action directe en soi. «La cryptographie est la forme par excellence de l'action directe non violente», a écrit Julian Assange[34].

Ajoutons que l'inaction politique a un coût. Quand la philosophie politique libérale, qui passe par le débat, les réformes et la médiatisation des enjeux, prévaut sur l'action directe, on peut se demander d'où peut venir le changement si le gouvernement décide de faire la sourde oreille. La société contemporaine accorde une grande valeur à la transparence et au débat public, souvent considérés comme le meilleur moyen de créer une pression politique capable d'amener des changements. Le fait que l'information soit accessible au public et puisse être matière à débat représente certes un acquis précieux, mais, pour que celle-ci puisse avoir une véritable portée

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

politique, il faut qu'elle puisse parfois entraîner des actes de sorte qu'elle génère une exigence incontournable[35].

La désobéissance civile est une façon de parvenir à cette fin. Elle peut donner à une bonne partie de la population (ces citoyens que le cadre politique libéral dessert ou laisse sans voix, ou encore les minorités qui, quoi qu'on en pense, ont un accès limité à la sphère publique) les moyens de contribuer directement au processus politique. Pour le politologue Robin Celikates, qui s'est penché sur la question, «les formes ponctuelles, informelles, extra-institutionnelles ou anti-institutionnelles d'action politique permettent aussi aux citoyens de contester et de participer, alors que les canaux institutionnels officiels d'action et de communication leur sont inaccessibles ou à tout le moins ne leur permettent pas de faire entendre adéquatement leurs doléances[36]».

Certains désapprouvent le recours à la désobéissance civile par une minorité. Après tout, si l'opinion défendue est marginale, c'est peut-être parce qu'elle est indésirable. Mais il s'agit là d'une analyse trompeuse. Même lorsqu'elle porte ses fruits, la désobéissance civile ne vise qu'à attirer l'attention sur une position politique – une position qui, pour se muer en une revendication capable d'ébranler le consensus dominant, devra d'abord être adoptée par un très grand nombre de citoyens. Les idées de Chelsea Manning, de Jeremy Hammond ou d'Edward Snowden, par exemple, n'étaient guère connues avant que ceux-ci les répandent en commettant des actes courageux et fassent ainsi des émules. (Notons qu'au moins un autre lanceur d'alerte aurait divulgué des documents relatifs à la NSA sur diverses plateformes[37], et que Phineas Fisher se serait inspiré des actions d'Anonymous contre des firmes de sécurité informatique.) Anonymes ou non, les actes courageux de ce genre amènent des gens à mettre en doute leur complaisance à l'égard de l'ordre établi, voire à y renoncer. Autrement dit, la désobéissance civile crée un contexte propice au développement de mouvements citoyens plus vastes.

Anonymous illustre parfaitement cette logique. Seule une minorité d'Anons pratiquent le *doxing*, le hacking ou les attaques par saturation, mais cela incite des spectateurs ou d'autres participants à s'activer – y

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

compris ceux qui désapprouvent leurs méthodes ou leurs effets[38]. Pourtant la question de la responsabilité d'Anonymous est aussi soulevée sur ce front par certains critiques. Bon nombre défendent en effet le recours à la désobéissance civile pour certains mouvements sociaux, mais la trouvent illégitime si dépourvue du sceau d'une entité juridiquement reconnue, bref, si elle est non légitimée par un risque de sanction. Comme le soutient Molly Sauter, cette conception de la désobéissance civile me semble étroite: elle est «profondément enracinée dans le concept chrétien de martyre et présuppose une supériorité morale du participant à un acte de désobéissance civile non violent sur ses adversaires. [...] En martelant que les hackers militants courent souvent le risque d'être sévèrement punis par l'État pour leur militantisme, on s'assure d'y attirer uniquement les gens dont les opinions sont les plus extrémistes ou qui ont le moins à perdre (c'est-à-dire ceux qui sont le moins intégrés à la société)[39]».

Tandis qu'Anonymous continue à faire part de ses revendications à l'État, à lutter contre la corruption et à soutenir d'autres militants dans leurs combats politiques, le collectif essaie de décoloniser une subjectivité aux habitudes bien enracinées: il ose viser un bien commun qui soit libéré des enjeux de la reconnaissance personnelle et de l'autopromotion. Après tout, beaucoup d'Anons sont des citoyens respectueux de la loi, qui pourraient s'attendre à voir leurs efforts récompensés par un minimum de célébrité. Or ils préfèrent invoquer leur «droit à l'opacité», pour reprendre la formule d'Édouard Glissant[40]. Le masque, souvent perçu de façon uniquement péjorative (comme vecteur de déresponsabilisation, de dissimulation), peut aussi donner lieu à une éthique constructive de l'interaction et de l'être-au-monde qui s'oppose aux intérêts de l'État, de la grande entreprise et de la puissance coloniale. D'ailleurs, ce droit matérialise un ensemble de refus motivés par des principes: refus de laisser l'État espionner ses citoyens, refus de laisser la grande entreprise marchandiser les communications personnelles et manipuler les désirs des gens, refus de tirer profit du travail d'autrui... des refus qui visent essentiellement à empêcher une idée formidable de s'évanouir: nous sommes anonymes et avons le droit de l'être.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Remerciements

MÊME SI LE TERRITOIRE VASTE et complexe qu'ont créé les militants d'Anonymous ne peut se ramener à un seul concept, une métaphore m'est constamment revenue à l'esprit pendant la rédaction de ce livre: le labyrinthe. Toute tentative de franchir, de comprendre ou de décrire une situation donnée ne faisait que dégrader l'énergie communicative qui s'en dégageait; quiconque y aurait participé ou l'aurait simplement observée aurait vécu une expérience distincte. C'est pourquoi ma recherche sur Anonymous a été une expérience certes palpitante, mais non moins éprouvante. J'ai passé des années à rassembler trop d'informations en tentant de bâtir le labyrinthe par lequel j'espérais trouver l'itinéraire qui me mènerait à celui des Anons. Toutefois, dès que j'entreprenais d'en démêler l'écheveau, de tisser un récit cohérent et limpide à partir des innombrables histoires, rumeurs, conversations et secrets que j'avais accumulés, je réalisais avec horreur que le résultat, fragile, s'effilochait entre mes doigts. Je m'étais égarée dans les ténèbres entre les sentiers; privée de repères, j'ignorais où se trouvait la sortie. Heureusement, un certain nombre d'amis, de collègues, d'inconnus et d'Anons m'ont aidée à m'orienter et m'ont encouragée, contribuant ainsi à ce que cette odyssée finisse par déboucher sur un livre.

Je m'étais lancée dans un travail de longue haleine. Ses balbutiements remontent à 2006-2007, alors que j'étais bénéficiaire d'une bourse de recherche postdoctorale à l'université de l'Alberta. J'ai eu la chance d'y

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

rencontrer le professeur Stephen A. Kent, qui, à titre de sociologue, administre le plus important fonds d'archives du monde sur l'Église de scientologie. Au cœur d'un hiver épouvantablement froid, je m'étais plongée dans cette documentation en ayant en tête de concrétiser un modeste projet parallèle sur une affaire que les geeks appellent «Internet contre Scientologie». J'étais plus habituée à réaliser des entretiens qu'à interpréter des piles de documents (qui, dans ce cas, s'avéraient particulièrement étranges). Fort heureusement, Kent m'a généreusement accompagnée dans l'exploration des entrailles de cette organisation déconcertante, fascinante et parfois inquiétante que tant de geeks se plaisent à dénigrer.

En janvier 2008, mes recherches historiques ont fait un bond dans le présent: en pleine campagne contre l'Église de scientologie, Anonymous avait subi une étonnante métamorphose, passant d'une bande d'effroyables joueurs de tours à un groupe d'activistes impétueux. J'étais conquise. Dès lors, il m'a semblé tout naturel de suivre ces fous pour voir si leur irruption franche et inattendue dans la culture de la contestation aurait des effets concrets – ce qui allait être le cas. Je vivais alors à New York. J'ai pu y découvrir Anonymous par l'entremise de sa turbulente cellule locale, qui m'accueillait dans ses manifestations mensuelles. De mon côté, j'invitais des Anons à participer à mes cours. Mes étudiants et moi avons ainsi pu profiter de leurs éloquents exposés sur la signification politique d'Anonymous et de leurs numéros sur les subtilités du *lulz*. En de nombreuses occasions, j'ai eu la chance de rencontrer ces interlocuteurs brillants que sont Little Sister, Sethdood et Matthew Danziger, dit PokeAnon. Sethood et PokeAnon ont d'ailleurs accepté de m'accorder des interviews en bonne et due forme. J'ai aussi eu le bonheur de faire connaissance avec les membres de Chanology Dublin et d'autres Anons irlandais, qui ont compté parmi mes professeurs les plus intrépides. J'ai traversé l'Atlantique à maintes reprises pour tirer parti de cette précieuse ressource. Lors de mon troisième voyage en trois ans, il était manifeste que certains d'entre eux – en particulier Pete, David, Firefly et Donncha –

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

n’étaient plus seulement des sources: ils étaient devenus des amis. Il me tarde de les revoir.

En 2010, alors qu’Anonymous se faisait connaître du grand public par sa campagne contre le blocage du financement de WikiLeaks, je me trouvais par hasard dans une année sabbatique, dans un sanctuaire: l’institut des études avancées de l’université Princeton. Sans la surabondance de temps dont je disposais, j’aurais été incapable de suivre la cascade d’activités du réseau AnonOps. Des discussions avec deux collègues de mon groupe, Manu Goswami et Tanya Erzen, m’ont aidée à donner forme à mes idées sur le sujet. L’anthropologue Didier Fassin a aussi été un mentor inspirant. Sa générosité sans bornes en termes de commentaires édifiants m’a été confirmée récemment, alors que je présentais un exposé sur Anonymous dans le cadre d’un atelier d’ethnographie de l’institut.

Fin 2010-début 2011, je me suis perdue dans le labyrinthe polymorphe d’Anonymous. Dans certaines zones, j’avançais sans savoir où j’allais, sans but; dans d’autres recoins, je cherchais assidûment à remplir une mission. J’y ai rencontré des dizaines de participants généreux de leur temps, de leur expérience, de leurs intuitions et de leur sens critique. Je les remercie tous en les implorant de pardonner mon incapacité à citer tous leurs noms – vrais, faux ou pseudos. Certains d’entre eux méritent une mention particulière, car ils n’ont reculé devant aucun effort pour me guider. Trivette, meddle et n0pants se sont empressés de m’accorder des entretiens privés. Ce faisant, ils m’ont ouvert plusieurs portes. Je me suis sentie bienvenue sur les canaux IRC #reporter, #freedommods et, plus tard, #cabincr3w. Toujours animées et éclairantes, les discussions y duraient des heures. Au fil du temps, d’autres Anons m’ont amenée à emprunter de nouvelles pistes de réflexion. Débordant d’énergie, Anoymous9 a été une source d’aide inépuisable; sans lui, jamais ce livre n’aurait vu le jour (du moins sous cette forme). m0rpeth a sans doute été un des premiers initiés à m’avoir imploré de cesser d’avaler les salades qu’on me servait parfois; par ses diatribes contre les structures de pouvoir qui prenaient forme au sein du collectif, il m’a aidé à comprendre celles-ci et, ce faisant, à découvrir les divers courants de la critique interne chez les Anons. Actif à différentes

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

époques et dans une diversité de contextes, blackplans a fait montre d'une vaste érudition et d'une grande vivacité d'esprit à l'égard d'Anonymous et de l'univers des hackers (sans parler de la vie en général). Loin d'être anonyme et d'être un fan d'Anonymous, Andrew Auernheimer m'en a appris beaucoup sur le trollage – souvent avec des arguments et des déclarations dignes d'un troll (fort heureusement, il ne m'a jamais trollée!). De nombreux Anons ont longuement chatté avec moi, dont c0s, AnonyOps, Barrett Brown, evilworks, q, mr_a, sharpie, Katanon, shitstorm, owen, Avunit, emmi, Jackal, p0ke, crypt0anonymous, Nicole Powers, Nixie, Commander X, JMC, papersplx, Lauri Love et plusieurs autres qui ont préféré garder l'anonymat.

Peu à peu (et en raison d'une série d'arrestations), le contexte dans lequel se passaient mes recherches a changé, tout comme la façon dont le public percevait mon objet d'étude. De nombreux Anons ont vécu de dures batailles judiciaires et ont séjourné en prison. Vu les difficultés qu'ils ont éprouvées, je les remercie d'autant plus d'avoir pris le temps de m'aider. Jamais je n'aurais pu terminer ce livre sans la générosité et la perspicacité de Jeremy Hammond, de Mustafa Al-Bassam, de Donncha O'Cearbhaill, de Darren Martyn et de Mercedes Haefer, qui ont tous consacré des heures à répondre à d'interminables séries de questions parfois répétitives. Chris Weatherhead et Jake Davis m'ont aussi fait part, en personne, de bon nombre de leurs expériences; Ryan Ackroyd, avec qui je n'ai commencé à discuter que récemment, m'a fait part de ses brillantes réflexions sur la «machine de haine d'internet» et les taupes.

Au cours de mes recherches, j'ai souvent chatté avec des journalistes et des cinéastes qui, comme moi, consacraient beaucoup de temps et d'énergie à tenter de reconstituer le puzzle Anonymous. Leur présence était la bienvenue: nos échanges, où nous parlions boulot et troquions nos notes, m'ont souvent procuré un drôle de soulagement et ont représenté un apport inestimable sur le plan professionnel. Mes discussions avec Quinn Norton, Asher Wolf, Steve Ragan et Brian Knappenberger ont largement contribué à mes réflexions sur Anonymous. Steve Ragan mérite une mention spéciale pour avoir si spontanément partagé ses connaissances avec moi; la plupart

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

des journalistes sont nettement plus avares de leurs informations. Le documentaire de Knappenberger et le reportage captivant de Parmy Olson sur Anonymous et LulzSec ont aussi été de précieuses ressources pour ce projet.

En 2013, plusieurs de mes collègues ont lu les premiers chapitres du livre et m'ont fait de judicieux commentaires: Danielle Citron, Nathan Schneider, Jonathan Sterne, Darin Barney, Christine Ross, Carrie Rentschler, Sandra Hyde, Michael Ralph, Whitney Phillips et Chris Kelty. Au fil des ans, j'ai donné d'innombrables conférences sur Anonymous, et je ne saurais rendre compte de l'abondance de commentaires que j'ai reçus; néanmoins, ceux de Paul Eiss, d'Angela Zito, de Faye Ginsburg, de Haidy Geismar, de Daniel Miller, d'Alberto Sanchez et de Bob Rutledge méritent d'être soulignés.

À l'Université McGill, j'ai la chance d'occuper un poste qui me permet à la fois de faire rayonner mes travaux et d'écrire. Je suis profondément reconnaissante au généreux donateur qui assure son financement. McGill est un milieu stimulant; je remercie particulièrement les participants au groupe de lecture Bits, Bots and Bytes, qui contribuent à un forum de recherche et à des échanges érudits que j'attends chaque mois avec impatience. Deux de ses membres, Scott Kushner et Elena Razlogova, ont lu des documents qui ne faisaient pas partie du programme et les ont commentés avec intelligence. Mon infatigable assistante de recherche, l'étudiante de premier cycle Maya Richmond, a réussi à dénicher chaque document que je lui ai demandé et m'a fait part de ses réflexions pertinentes sur les hackers et les *tricksters*. Caroline Habluetzel, qui a obtenu son doctorat dans notre département, a aussi été une précieuse et méticuleuse assistante de recherche. Elle combattait alors un cancer, qui a finalement eu raison d'elle en mai 2013. Elle nous manque beaucoup. J'ai fait lire un premier jet des cinq premiers chapitres du livre aux étudiants inscrits à mon cours de cycle supérieur intitulé «Les enfers technologiques», ce qui a donné lieu à des questionnements intéressants et à la détection de plusieurs problèmes. Darcie DeAngelo a dépassé mes attentes en les commentant de manière approfondie. Molly Sauter était alors en train de terminer le

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

manuscrit de son propre livre (*The Coming Swarm: DDOS Actions, Hacktivism, and Civil Disobedience on the Internet*), dont la lecture s'est avérée tout aussi essentielle que passionnante à cette étape où je m'interrogeais sur l'éthique de l'action directe numérique.

Écrire un ouvrage destiné au grand public tout en restant fidèle aux détails d'ordre technique et juridique, souvent complexes et ésotériques, représente tout un défi. J'ai demandé conseil à plusieurs experts pour m'assurer de bien rendre ces nuances. Orin Kerr, Marcia Hoffman, Ahmed Ghappour et Andres Guadamuz ont examiné les passages juridiques. Plusieurs technologues et hackers ont inlassablement répondu à mes nombreuses questions: David Mirza, Chris Soghoian, Dino A. Dai Zovi, Chris Wysopal, Space Rouge, James Atkinson, Patrick Gray, Dan Guido, Morgan Marquis-Boire et Brian Martin. Aussi, les journalistes Kim Zetter et Ted Bridis ont dissipé des incertitudes que j'entretenais à propos des hackers et des politiques du Federal Bureau of Investigation (FBI) relatives aux informateurs. Toute imprécision qui aurait subsisté doit être imputée à mon incapacité à suivre les excellents conseils de ces consultants.

Je dois remercier les membres de ma famille d'avoir su endurer les effets de mon travail de rédaction; les Anderson se sont montrés patients et bienveillants pendant les trois dernières périodes des Fêtes, alors que je n'étais pas aussi présente que les autres. Fan inconditionnel de mon travail, mon père a veillé à ce que ses amis, retraités pour la plupart, apprennent des choses cruciales sur Anonymous. Enfin, mon chien Roscoe, avec sa charmante dent de travers, a su chaque jour m'éloigner du bureau, ce qui m'a permis de prendre des pauses, essentielles.

Trois personnes ont laissé leur empreinte sur l'ensemble de ce livre, qu'elles ont lu du début à la fin (et plus d'une fois pour deux d'entre elles). Mon conjoint Mitch Anderson, qui passe ses journées (et, trop souvent, ses nuits) à gérer un fournisseur d'accès internet respectueux de la vie privée de sa clientèle, est un rédacteur talentueux. Après avoir lu les premiers chapitres, il m'a prise entre quatre-z-yeux pour me faire comprendre que je devrais adopter un ton plus vivant et décrire davantage si j'entendais publier un ouvrage destiné au grand public. Ensuite, ses lectures de chacun des

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

chapitres lui ont inspiré des remarques et modifications qui m'ont été utiles. Il a notamment arrosé d'essence toutes mes tentatives de faire de l'humour avant d'y mettre le feu avec ses propres blagues. Certaines plaisanteries étaient trop cruelles ou trop imaginatives, si bien que j'ai dû jeter un seau d'eau sur le brasier, mais les choses étaient néanmoins nettement mieux qu'au départ. Je lui suis infiniment reconnaissante d'avoir accepté de participer au processus créatif et de m'avoir soutenue pendant que j'écrivais deux livres d'affilée – ce que je ne referai jamais.

En partie à cause des conseils de Mitch (et en partie à cause de ma tendance à vouloir tout expliquer), j'ai complètement dépassé les limites que je m'étais fixées en écrivant trop. Deux personnes ont su réfréner mes ardeurs, relever mes incohérences, m'ont aidée à élaguer le manuscrit et ont fait tout leur possible pour le bonifier.

D'abord, mon assistant de recherche Matt Goerzen, artiste aussi excentrique que talentueux et spécialiste des questions d'anonymat, a été mon relecteur de première ligne. Journaliste de métier, Matt est un rédacteur habile qui sait apporter une touche de grâce et de clarté à tous les textes qu'il croise. Nourris par ses recherches sur les cultures de l'anonymat, ses commentaires ont été excellents. Ce livre a largement profité de sa volonté de lui insuffler sa sagesse. Je lui serai éternellement redevable d'avoir été mon guide le plus fidèle, et je ne peux qu'espérer pouvoir lui rembourser ma dette en dirigeant son mémoire de maîtrise.

Parmi les maisons d'édition potentielles, je souhaitais en trouver une qui puisse m'aider à trouver le juste équilibre entre profondeur d'analyse et accessibilité. Verso s'est immédiatement révélée comme la candidate numéro un, et j'ai eu grand plaisir à travailler avec toute son équipe, dont Mark Martin, Colin Beckett, Jennifer Tighe et Jacob Stevens. J'ai particulièrement apprécié ma collaboration avec Andrew Hsiao. Je savais mon manuscrit beaucoup trop long, et j'avoue avoir redouté qu'Andrew y effectue des coupes draconiennes, mais ses suggestions se sont avérées à tel point brillantes et précises que l'émondage a été beaucoup moins douloureux que prévu. Andrew a passé le manuscrit au peigne fin. Très pointilleux sur les détails de la formulation, il a su tenir compte de la valeur

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

de mes arguments et prendre le recul nécessaire pour circonscrire les phrases, les sections ou même les chapitres où s’imposait un coup de rasoir. À maintes reprises, s’il avait été possible d’embrasser les gens par courriel, je ne m’en serais pas privée. J’ai aussi beaucoup apprécié nos discussions sur l’édition et la politique, et j’espère que nous en aurons d’autres à l’avenir.

Enfin, j’aimerais remercier tous les militants, garnements, plaisantins et autres clowns masqués pour leur mise en scène de ce récit épique et pour m’avoir offert l’occasion d’écrire à son sujet.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Remarque sur les sources

Ce livre, qui propose une ethnographie populaire d'Anonymous, repose largement sur les méthodologies, conventions et gestion des sources propres au journalisme. Parce que la duplicité, le mensonge et l'invention sont les instruments de «travail» (souvent maniés avec fierté) de ceux et celles qui se revendiquent d'Anonymous, de nombreux lecteurs se demanderont comment les informations qui se trouvent dans ce livre peuvent être vérifiées. Certes, la véracité de certaines anecdotes est impossible à valider ou ne s'appuie que sur des journaux de chat. Mais elles viennent se greffer à des faits largement documentés par des sources judiciaires. Ce livre n'aurait d'ailleurs sans doute pu voir le jour si l'identité de nombreux participants n'avait été divulguée après leur arrestation et les poursuites dont ils ont fait l'objet, et sans le trésor d'informations (parfois problématiques) rendues publiques par les autorités. De plus, si, par sa nature même, l'anonymat permet à des individus de dénoncer de puissantes institutions, ceux qui sont arrêtés et condamnés découvrent soudain une autre forme de liberté: celle de s'exprimer en toute transparence sur leur identité et leur parcours individuel, émancipés des limites du pseudonyme collectif ou protecteur. En ayant accès aux journaux de chat et, en particulier, aux documents judiciaires, j'ai pu vérifier beaucoup d'affirmations faites par des Anons et d'autres participants avant leur arrestation. (Dans l'immense majorité des cas, leurs dires ont été confirmés.) Les journaux de chat cités dans ce livre proviennent de diverses

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

sources, soit de canaux Internet Relay Chat (IRC) publics, de journaux publiés en ligne par Anonymous, de journaux privés qu'on m'a remis, ou encore de journaux déposés comme preuve devant les tribunaux et communiqués à des journalistes. Dans les cas où aucun document n'était disponible, j'ai tenté d'interviewer plusieurs participants et me suis fiée, lorsque c'était possible, à des reportages publiés par des journalistes reconnus. Malheureusement, j'ai dû exclure des pages de ce livre bon nombre d'anecdotes et de personnages intrigants dont l'existence ne reposait que sur des rumeurs. Parce que bon nombre des gens dont il est ici question sont maintenant connus du public (et qu'on a abondamment écrit sur eux), je n'ai pas modifié leurs noms ou leurs pseudos, sauf si la révélation de leur identité constituait une prise de risques pour eux.

Ce livre doit être lu comme un recueil d'expériences et de réflexions personnelles. Bien que j'y aborde des événements importants, et ce qui pourrait être qualifié de tournants historiques, et que j'aie tenté d'y inclure des points de vue divers (et parfois conflictuels), il est nécessaire de souligner qu'il se passe considérablement plus de choses au sein d'Anonymous que ce qu'on découvre dans ces pages.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Glossaire

Anon: Membre du collectif Anonymous; de l'abréviation d'«anonyme», «anon.», qui apparaît par défaut lorsqu'aucun pseudo n'est choisi par le participant à un forum.

Attaque informatique par saturation, attaque par déni de service, DDoS (*distributed denial of service*): Attaque informatique consistant à envoyer, à partir de dizaines d'ordinateurs, des milliers de requêtes à un serveur dans le but de le paralyser et, ce faisant, d'en bloquer l'accès aux internautes.

Black hat: L'appellation francisée «chapeau noir» a cours, mais est peu usitée. Hacker menant des activités illégales dans un but délibérément malveillant.

Botnet: Ensemble d'ordinateurs personnels mis au service d'une opération de hacking, avec ou sans la permission de leurs propriétaires; lorsque les ordinateurs sont mobilisés à l'insu de leurs propriétaires, on qualifie le *botnet* de «réseau de (machines) zombies».

Défaçage, défacer: Opération de hacking consistant à modifier la page d'accueil du site web d'une organisation.

Doxer (v.), *doxing* (n.): Opération de hacking consistant à divulguer des renseignements personnels (nom, coordonnées, etc.) ou d'autres données privées qui se trouvent sur le serveur d'une organisation.

Exploit (prononcer à l'anglaise): Introduction dans un système informatique par exploitation de ses vulnérabilités.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Fag; *-fag* (suffixe); *faggotry*; *-faggotry* (suffixe): Catachrèses des mots anglais *fag* et *faggotry*, qui signifient pédé et homosexualité (avec une forte connotation négative), employées par les hackers comme qualificatif ou suffixe péjoratif. Exemple: *newfag* pour néophyte, *moralfag* pour hacker obéissant à des principes éthiques, *leaderfag* pour quelqu'un qui tente de prendre la direction d'une opération.

Faussaire: En anglais, *hoaxer.* Internaute qui monte et répand un canular (*hoax*) en ligne.

Gamer: Adepte des jeux vidéo.

Geek: Passionné d'informatique ou de tout ce qui est high-tech.

Gray hat: L'appellation francisée «chapeau gris» a cours, mais est peu usitée. Hacker qui n'hésite pas à agir dans l'illégalité, mais uniquement dans le but de détecter des vulnérabilités et de les faire connaître. Le *gray hat* occupe une position ambiguë, entre celles des *black hats* mal intentionnés et des *white hats* bien intentionnés.

Griefer: Troll qui sévit dans les jeux collaboratifs en ligne.

Hacker (v.), hacker (n.), hacking (n.): Activité consistant à s'introduire, par curiosité ou par goût du défi, dans un système ou un réseau informatique. Le hacking ne procède pas nécessairement d'intentions malveillantes (lorsque c'est le cas, on parle de hacking *black hat* ou de piratage).

Imageboard: Forum internet reposant essentiellement sur le partage d'images.

Journal: En anglais, *log*. Historique des événements qui se déroulent dans un processus informatique; par extension, fichier qui contient cet historique.

Leet speak: Système d'écriture utilisant les caractères alphanumériques ASCII, prisé des geeks. Exemple: *1337 5P34K* pour *leet speak.*

Lol: Acronyme de *laughing out loud* (rire aux éclats), employé en argot internet ou dans les SMS; les francophones écrivent parfois «mdr» (mort de rire).

Lulz: État d'esprit propre à l'humour noir des Anons; dérivé de *lol*.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Mème internet: Image, vidéo ou formule très brève et humoristique diffusée sur internet par l'entremise des médias sociaux.

Nerd: Passionné de science ou de nouvelles technologies.

Omg: Acronyme de *oh my God!* (mon Dieu!).

Pastebin: Site où l'on copie des lignes de code ou des textes trop longs pour être directement cités dans un échange sur un forum de discussion.

Phile: Dérivé de *textfile*. Fichier texte contenant spécifiquement des instructions pour réaliser des mauvais coups – de hacking ou de *phreaking*, ou encore une recette pour préparer du poison, une tactique terroriste, etc.

Phone phreak, phreaker, phreaking: Opération consistant à s'introduire illégalement dans un système téléphonique en reproduisant les fréquences audio employées pour l'acheminement des appels, à la fois par curiosité et dans un esprit de transgression.

Réseau de (machines) zombies: Voir *botnet.*

rm -rf: Dans un système d'exploitation UNIX (dont OS X et les systèmes à noyau Linux), commande à l'aide de laquelle un superutilisateur supprime l'ensemble d'un répertoire.

Rootkit: Mallette à outils de dissimulation d'activité employée par le hacker. Une fois installés sur l'ordinateur cible, ces programmes furtifs permettent à ce dernier d'effacer ses traces et de conserver un accès administrateur permanent au système d'exploitation visé afin d'y dissimuler d'autres programmes.

Ruche (mode): Lors d'une attaque par saturation, mode permettant à des ordinateurs de contribuer automatiquement à un *botnet* volontaire.

Skiddie: Terme employé par les hackers pour désigner les prétendus programmeurs dépourvus de compétences solides.

Sniffer (v.): Technique appelée également «analyse de paquet» et consistant à détecter et à enregistrer des paquets de données en circulation, notamment les mots de passe des abonnés d'un système.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Spool: Dans un système informatique, file d'attente où sont placées des informations avant d'être récupérées par leur destinataire ou acheminées à un périphérique. Exemple: boîte de courriel, serveur d'impression.

Trickster: Parfois appelé en français «fripon» (traduction française des travaux de Paul Radin), «farceur», «décepteur» (Claude Lévi-Strauss). Personnage mythique, dont les caractéristiques sont d'être espiègle, malicieux, désordonné et imprévisible, présent sous différents noms dans toutes les cultures.

Troll: Internaute qui intervient dans le seul but de nuire en soulevant la polémique, souvent en insultant des groupes ou des individus, pour le simple plaisir de la chose.

Troll train: Groupe de trolls qui se sont coordonnés pour une opération.

VPN: Abréviation de l'anglais *virtual private network*, réseau privé virtuel. Réseau informatique qui, grâce à des tunnels virtuels utilisant internet, permet de transmettre des données protégées grâce au chiffrement ou à l'encapsulation.

White hats: L'appellation francisée «chapeau blanc» a cours, mais est peu usitée. Expert en sécurité informatique qui effectue des tests d'intrusion dans des systèmes informatiques en vue d'y déceler des vulnérabilités et d'en avertir les propriétaires en cas de problème.

Wiki: Site web collaboratif au contenu duquel tout internaute peut contribuer.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Notes

Notes de l'avant-propos

[1] «Dear Fox News», vidéo YouTube, publiée par dearfoxnews, 29 juillet 2007, www.youtube.com/watch?v=RFjU8bZR19A.

[2] Citation extraite d'une conférence donnée en classe.

[3] «Message to Scientology», vidéo YouTube, publiée par Church0fScientology, 21 janvier 2008, www.youtube.com/watch?v=JCbKv9yiLiQ.

[4] Siobhan Gorman, «Alert on Hacker Power Play», *Online.wsj.com*, 21 février 2012.

[5] Sam Biddle, «No, Idiots, Anonymous Isn't Going to Destroy the Power Grid», *Gizmodo.com*, 21 février 2012.

Notes du chapitre 1

[1] Certains pseudos ne prennent pas la majuscule, usage que nous avons respecté. [NdT]

[2] Danielle Keats Citron, *Hate 3.0: The Rise of Discriminatory Online Harassment and How to Stop It*, Cambridge (MA), Harvard University Press, à paraître; Danielle Keats Citron, «Cyber Civil Rights», *Boston University Law Review*, vol. 91, 2009.

[3] Pour une critique en profondeur de la CFAA et des recommandations en vue de la réformer, voir www.eff.org/issues/cfaa.

[4] Tom McCarthy, «Andrew Auernheimer's Conviction over Computer Fraud Thrown Out», *The Guardian*, 11 avril 2014.

[5] Joseph Carey, message Twitter, 22 juillet 2013, 10 h 22, http://twitter.com/JDCarey Music/status/359362756568285184.

[6] weev, «I am weev. I may be going to prison under the Computer Fraud and Abuse Act tomorrow at my sentencing. AMA», reddit, 17 mars 2013, www.reddit.com/r/IAmA/comments/1ahkgc/i_am_weev_i_may_be_going_to_prison_under_the/c8xgqq9.

[7] Daniel Bates, «Standing by Her Man: Strauss-Kahn's Wife Puts Her Mansion Up as Collateral to Get Him out of Jail and She's Paying the Rent at His "Golden Cage"», *Daily Mail*, 21 mai 2011.

[8] «*Lulz*», *Encyclopedia Dramatica*, http://encyclopediadramatica.es/Lulz.

[9] On peut voir les premières mentions de «*lulz*» sur le site LiveJournal de Jameth: www.livejournal.com/users/jameth.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

[10] Whitney Phillips, «LOLing at Tragedy: Facebook Trolls, Memorial Pages and Resistance to Grief Online», *First Monday*, vol. 16, nº 12, 2011.

[11] Phrase prononcée par les enfants lors de la fête d'Halloween, qui signifie littéralement «Vous me donnez des bonbons ou je vous jette un mauvais sort». [NdT]

[12] La plupart de ces réflexions sont délicieusement approfondies par Lewis Hyde dans son ouvrage magistral intitulé *Trickster Makes This World: Mischief, Myth, and Art*, New York, Farrar, Straus and Giroux, 1998.

[13] *Ibid.*, p. 9.

[14] Alexander R. Galloway et Eugene Thacker, *The Exploit: A Theory of Networks*, Minneapolis, University of Minnesota Press, 2007.

[15] Phil Lapsley, *Exploding the Phone: The Untold Story of the Teenagers and Outlaws Who Hacked Ma Bell*, New York, Grove, 2013, p. 226.

[16] Steven Levy, *L'éthique des hackers*, Paris, Globe, 2013.

[17] Adam L. Penenberg, «A Private Little Cyberwar», *Forbes*, février 2000.

[18] «Biography of u4ea», *SoldierX*, www.soldierx.com/hdb/u4ea.

[19] Marco Deseriis, «"Lots of Money Because I Am Many": The Luther Blissett Project and the Multiple-Use Name Strategy», dans *Cultural Activism: Practices, Dilemmas and Possibilities*, Amsterdam, Rodopi, 2011, p. 65-93.

[20] Trond Lossius, «/55\[Fwd: [max-msp] it's over]», liste de diffusion /55\, 15 janvier 2001, www.bek.no/pipermail/55/2001-January/000102.html. On peut avoir un bon aperçu des œuvres de Nezvanova sur www.nettime.org/Lists-Archives/nettime-bold-0009/msg00073.html.

[21] Lee Knuttila, «Users Unknown: 4chan, Anonymity and Contingency», *First Monday*, vol. 16, nº 10, octobre 2011.

[22] Phillips, «LOLing at Tragedy», *loc. cit.*

[23] David Graeber, «Manners, Deference, and Private Property in Early Modern Europe», *Comparative Studies in Society and History*, vol. 39, octobre 1997, p. 694-728.

[24] Christopher Kelty, *Two Bits: The Cultural Significance of Free Software*, Durham (NC), Duke University Press, 2008.

Notes du chapitre 2

[1] Anonymous, «The Story Behind the Tom Cruise Video Link», *Why We Protest*, 27 juillet 2013, http://whyweprotest.net/community/threads/the-story-behind-the-tom-cruise-video-leak.93170/page-4.

[2] «The Cruise Indoctrination Video Scientology Tried to Suppress», *Gawker*, 15 janvier 2008.

[3] L. Ron Hubbard, «Comment faire en sorte que la Scientologie continue à fonctionner», dans *Cours d'auditeur solo*, s.l., Église de scientologie, 24 février 2015.

[4] L. Ron Hubbard, «Scientology Technology», *The Auditor*, nº 41, 1968.

[5] XENU TV, «The Story Behind the Tom Cruise Video Link», *Why We Protest*, 7 septembre 2011, http://whyweprotest.net/community/threads/the-story-behind-the-tom-cruise-video-leak.93170/page-3.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

[6] «Code of Conduct», vidéo YouTube, publiée par Church0fScientology, 1er février 2008, www.youtube.com/watch?v=-063clxiB8I.

[7] Cain, «Hal Tuner Raid Planned for Tomorrow», *The PFLD*, 20 avril 2007, http://episkoposcain.blogspot.ca/2007/04/hal-turner-raid-planned-for-tomorrow.html.

[8] Asterix, «August Theme: Anonymous Takes Back Chanology», *Why We Protest*, 14 juillet 2008, https://whyweprotest.net/threads/august-theme-anonymous-takes-back-chanology.18139/page-2.

[9] *Why We Protest*, http://whyweprotest.net/community/threads/false-press-we-need-to-deal-with-this-immediately.80242.

[10] «Operation Slickpubes», *Motherfuckery*, 10 janvier 2009, http://motherfuckery.org/this-is-how-a-post-looks.

[11] «In 2009, NYPD Issued "Surveillance Request" to "Identify" Anonymous Members During Their Anti-Scientology Rally», *Techdirt*, 4 septembre 2013, www.techdirt.com/articles/20130903/14213924394/2009-nypd-issued-surveillance-request-to-identify-anonymous-members-during-their-anti-scientology-rally.shtml.

[12] Eric J. Hobsbawn, *Les primitifs de la révolte dans l'Europe moderne*, Paris, Fayard, coll. «Pluriel», 2012, p. 23.

[13] *Ibid.*, p. 56.

[14] Tony Ortega, «Meet the Man Behind WWP, the Web Home of Anonymous and Project Chanology», *The Underground Bunker*, 22 juin 2013, http://tonyortega.org/2013/06/22/meet-the-man-behind-wwp-the-web-home-of-anonymous.

[15] Entretien en ligne avec l'auteure.

[16] Anonymous, «What the Dicks Is Marblecake and What Do They Do?», *Why We Protest*, 23 juillet 2008, https://whyweprotest.net/threads/what-the-dicks-is-marblecake-and-what-do-they-do.16012/page-13.

[17] Paolo Gerbaudo, *Tweets and the Streets: Social Media and Contemporary Activism*, Londres, Pluto, 2012.

[18] Jo Freeman, «The Tyranny of Structurelessness», *The Second Wave*, vol. 2, no 1, 1972, www.jofreeman.com/joreen/tyranny.htm.

[19] L. Ron Hubbard, *Penalties for Lower Conditions*, HCO Policy Letter, 18 octobre 1967, cité dans «The Fair Game Policy: The True Spirit of Scientology», *Operation Clambake*, www.xenu.net/fairgame-e.html.

Notes du chapitre 3

[1] David Leigh, «*Guardian* Gagged from Reporting Parliament», *The Guardian*, 12 octobre 2009.

[2] Christian Christensen, «Collateral Murder and the After-Life of Activist Imagery», *Medium*, 14 avril 2014, https://medium.com/@ChrChristensen/collateral-murder-and-the-after-life-of-activist-imagery-3fc2accd82bb#.c3rrl5k4l.

[3] Evan Hansen, «Manning-Lamo Chat Logs Revealed», *Wired*, 13 juillet 2011, www.wired.com/2011/07/manning-lamo-logs.

[4] Lamo prétend que le fait d'avoir publié quelques articles fait de lui un journaliste. Aussi, il a déjà prétendu être pasteur de la Universal Life Church (Église de la vie universelle). Voir Luis Martinez,

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

«Bradley Manning Accuser Adrian Lamo Takes the Stand», *ABC News*, 20 décembre 2011, http://abcnews.go.com/blogs/politics/2011/12/bradley-manning-accuser-adrian-lamo-takes-the-stand.

[5] Ed Pilkington, «Bradley Manning's Treatment Was Cruel and Inhuman, UN Torture Chief Rules», *The Guardian*, 12 mars 2012.

[6] Raffi Khatchadourian, «No Secrets», *The New Yorker*, 7 juin 2010.

[7] Le lien se révèle encore plus étroit lorsqu'on sait que, jeune, Julian Assange a lui-même tâté de la lutte contre la Scientologie. Alors qu'il vivait encore en Australie, il dirigeait un fournisseur de services internet, Suburbia, qui défendait la liberté d'expression et hébergeait des contenus anti-Scientologie. Il a aussi organisé une manifestation contre l'Église de scientologie à Melbourne en 1996.

[8] Wilford's Dog, «AMA Request Sabu from LuLSec (sic) This Would Be Amazing», reddit, 23 septembre 2011, www.reddit.com/r/IAmA/comments/kpfsp/ama_request_sabu_from_lulsec_this_would_be_amazing.

[9] Guest, «Untitled», *Pastebin*, 5 juillet 2010, http://pastebin.com/ytZ7N1x7.

[10] Par souci de confidentialité, l'adresse IP ici mentionnée est fictive.

[11] Pour en savoir plus sur les réseaux de zombies, voir l'excellent ouvrage de Finn Brunton intitulé *Spam: A Shadow History of the Internet*, Cambridge (MA), MIT Press, 2013.

[12] «Activists Target Recording Industry Websites», *BBC News*, 20 septembre 2010, www.bbc.com/news/technology-11371315.

[13] Ernesto, «Anti-Piracy Outfit Tries to Erase History», *TorrentFreak*, 15 octobre 2011, https://torrentfreak.com/anti-piracy-outfit-tries-to-erase-history-111015.

[14] David Kravets, «Wired Exclusive: I Was a Hacker for the MPAA», *ABC News*, 22 octobre 2007, http://abcnews.go.com/Technology/story?id=3760199.

[15] Enigmax, «Anti-Piracy Outfit Threatens to DoS Uncooperative Torrent Sites», *TorrentFreak*, 5 septembre 2010, https://torrentfreak.com/anti-piracy-outfit-threatens-to-dos-uncooperative-torrent-sites-100905.

[16] Enigmax, «4chan DDoS Takes Down MPAA and Anti-Piracy Websites», *TorrentFreak*, 18 septembre 2010, https://torrentfreak.com/4chan-ddos-takes-down-mpaa-and-anti-piracy-websites-100918.

[17] «Hackers Hit Hollywood's Piracy Watchdog», Reuters, 19 septembre 2010, http://ca.reuters.com/article/idCATRE68J09F20100920.

[18] Christopher Williams, «Piracy Threats Lawyer Mocks 4chan DDoS Attack», *The Register*, 22 septembre 2010.

[19] Nate Anderson, «"Straightforward Legal Blackmail": A Tale of P2P Lawyering», *Ars Technica*, 6 juin 2010, http://arstechnica.com/tech-policy/2010/06/straightforward-legal-blackmail-a-tale-of-p2p-lawyering.

[20] «Lords Hansard text for 26 Jan 201026 Jan 2010 (pt 0003)», site web du Parlement du Royaume-Uni, www.parliament.the-stationery-office.co.uk/pa/ld200910/ldhansrd/text/100126-0003.htm.

[21] Nate Anderson, «The "Legal Blackmail" Business: Inside a P2P Settlement Factory», *Ars Technica*, 28 septembre 2010, http://arstechnica.com/tech-policy/2010/09/amounts-to-blackmail-inside-a-p2p-settlement-letter-factory.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

[22] Enigmax, «ACS:Law (Gay) Porn Letters Target Pensioners, Married Men», *TorrentFreak*, 25 septembre 2010, https://torrentfreak.com/acslaw-gay-porn-letters-target-pensioners-married-men-100925.

[23] Charles Arthur, «ACS:Law and MediaCAT Close Their Doors, Ending Filesharing Claims», *The Guardian*, 4 février 2011.

[24] «ACS:Law Solicitor Andrew Crossley Suspended by SRA», *BBC News*, 18 janvier 2012, www.bbc.com/news/technology-16616803.

[25] Josh Halliday, «ACS:Law Solicitor at Centre of Internet Piracy Row Suspended», *The Guardian.com*, 18 janvier 2012.

[26] Ernesto, «Behind the Scenes at Anonymous' Operation Payback», *TorrentFreak*, 15 novembre 2010, https://torrentfreak.com/behind-the-scenes-at-anonymous-operation-payback-111015.

[27] «Anonymous Is Not Unanimous», *Pastebin*, http://pastebin.com/4vprKdXH.

[28] «PPi Ask Anonymous to Stop Payback», *Pirate Parties International – General Talk*, novembre 2010, http://lists.pirateweb.net/pipermail/pp.international.general/2010-November/008046.html.

[29] Partis pirates du Royaume-Uni et des États-Unis, «Pirate Party Op», *Scribd*, 19 novembre 2010, www.scribd.com/doc/43400303/Pirate-Party-OP.

[30] Ernesto, «Behind the Scenes at Anonymous' Operation Payback», *loc. cit.*

[31] Entretien en ligne avec l'auteure.

[32] *Ibid.*

[33] Pour un exemple, voir «Untitled», *Pastebin*, 24 février 2011, http://pastebin.com/0Y5CkrF9.

[34] Entretien en ligne avec l'auteure.

[35] *Ibid*.

[36] gster, «DDoS Attacks on Pro-Copyright Groups: Pirate Parties and "Operation Payback"», *Play Station Universe*, 25 novembre 2010, www.psu.com/forums/showthread.php/245537-DDoS-attacks-on-pro-copyright-groups-Pirate-Parties-and-Operation-Payback?p=5287480.

Notes du chapitre 4

[1] Art Keller, «Dozens (Yes, Dozens) Show Up for Anonymous' MillionMask March», *Newsweek*, 7 novembre 2013.

[2] Littéralement «porno de chats», mais il s'agit en fait de photos et de vidéos de chats, très populaires en ligne et qui n'ont rien de porno: le suffixe *-porn*, en anglais, en est venu à désigner tout site proposant un type d'images que les gens aiment regarder: *earthporn*, *mapporn*, *bookporn*, etc. [NdT]

[3] George Santayana, *Dominations and Powers*, New Brunswick (NJ), Transaction, 1995, p. 33.

[4] Henry Brooks Adams, cité dans Russ Marion, *The Edge of Organization: Chaos and Complexity Theories of Formal Social Systems*, Thousand Oaks (CA), SAGE, 1999, p. xii.

[5] Justin Elliot, «The 10 Most Important Wikileaks Revelations», *Salon*, 29 novembre 2010, www.salon.com/2010/11/29/wikileaks_roundup.

[6] Martin Beckford, «Sarah Palin: Hunt WikiLeaks Founder Like alQaeda and Taliban Leaders», *The Telegraph*, 30 novembre 2010.

[7] Kathryn Jean Lopez, «On This Sunday Outrage», *National Review*, 28 novembre 2010.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

[8] À l'époque, les statistiques se trouvaient sur http://searchirc.com/channel-stats et http://irc.netsplit.de/networks/top10.php (encore actif).

[9] Richard Stallman, «The Anonymous WikiLeaks Protests Are a Mass Demo Against Control», *The Guardian*, 17 décembre 2010.

[10] Pour des données précises, voir Molly Sauter, *The Coming Swarm: DDOS Actions, Hacktivism, and Civil Disobedience on the Internet*, Londres, Bloomsbury Academic, 2014.

[11] [Allusion aux batailles de Lexington et Concord, qui ont inauguré la guerre de l'Indépendance des États-Unis en 1775. Le coup en question a en fait eu lieu à Concord. (NdT)]. Noam Cohen, «Web Attackers Find a Cause in WikiLeaks», *The New York Times*, 9 décembre 2010; Barlow cite Ralph Waldo Emerson, «Hymne chanté à l'inauguration du monument de Concord le 9 avril 1836», dans *Les pages immortelles de Emerson choisies et expliquées par E. Lee Masters*, Paris, Corréa, 1947, p. 221.

[12] Parmy Olson, *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*, New York, Back Bay, 2013, p. 109.

[13] Sean-Paul Correll, «'Tis the Season of DDoS—WikiLeaks Edition», *PandaLabs Blog*, http://www.pandasecurity.com/mediacenter/news/tis-the-season-of-ddos-wikileaks-editio/.

[14] Sean-Paul Correll, «Operation:Payback Broadens to "Operation Avenge Assange"», *PandaLabs Blog*, http://www.pandasecurity.com/mediacenter/news/operationpayback-broadens-to-operation-avenge-assange/.

[15] Kurt Vonnegut, *Abracadabra*, Paris, Éditions de l'Olivier, 1992, p. 266.

[16] Nick Davies, «10 Days in Sweden: The Full Allegations Against Julian Assange», *The Guardian*, 17 décembre 2010.

[17] Michel de Certeau, *L'invention du quotidien*, t. 1, *Arts de faire*, Paris, Gallimard, 2012, p. xlvi, 48.

[18] Jon Snow, message Twitter, 9 décembre 2010, 5 h 22, https://twitter.com/jonsnowC4/status/12814239458656256.

[19] Zeynep Tufekci, «WikiLeaks Exposes Internet's Dissent Tax, Not Nerd Supremacy», *The Atlantic*, 22 décembre 2010.

[20] Entretien en ligne avec l'auteure.

[21] Mikhaïl Bakhtine, *Esthétique et théorie du roman*, Paris, Gallimard, 1978.

[22] Ethan Case, «The Dark Side of Anonymous: Everything You Never Knew About the Hacktivist Group», *Mic*, 3 janvier 2012, http://mic.com/articles/3106/the-dark-side-of-anonymous-everything-you-never-knew-about-the-hacktivist-group.

[23] «Untitled», *Pastebin*, 10 décembre 2010, http://pastebin.com/WzzJ1Jp3.

[24] Joel Johnson, «What Is LOIC?» *Gizmodo*, 8 décembre 2010, http://gizmodo.com/5709630/what-is-loic.

[25] Gerry Smith, «Feds Charge 13 Members of Anonymous in "Operation Payback" Attacks», *Huffington Post*, 3 octobre 2010, www.huffingtonpost.com/2013/10/03/anonymous-charges-operation-payback_n_4039887.html.

[26] La référence en matière de chronique des balbutiements du hacking activiste: Tim Jordan et Paul A. Taylor, *Hacktivism and Cyberwars: Rebels with a Cause?*, New York, Routledge, 2004

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

[27] Molly Sauter, «“LOIC Will Tear Us Apart”: The Impact of Tool Design and Media Portrayals in the Success of Activist DDoS Attacks», *American Behavioral Scientist*, vol. 57, nº 7, 2013, p. 983-1007.

[28] Frances Fox Piven, *Who's Afraid of Frances Fox Piven?: The Essential Writings of the Professor Glenn Beck Loves to Hate*, New York, New Press, 2011.

[29] Sauter, «“LOIC Will Tear Us Apart”», *loc. cit.*

[30] Elinor Mills, «Old-time Hacktivists: Anonymous, You've Crossed the Line», *CNET*, 30 mars 2012, www.cnet.com/news/old-time-hacktivists-anonymous-youve-crossed-the-line.

[31] Tod Gemüse, commentaire sur la page Facebook du Cult of the Dead Cow, 10 janvier 2013, www.facebook.com/groups/28828338908/permalink/10151344658883909.

[32] Pour un exposé approfondi et éclairant sur l'attaque par saturation en tant qu'intervention faisant avancer la cause de la liberté d'expression tout en constituant une forme d'action directe, voir Sauter, *The Coming Swarm*, *op. cit*.

[33] Ethan Zuckerman *et al.*, *2010 Report on Distributed Denial of Service (DDoS) Attacks*, Berkman Center for Internet and Security, 20 décembre 2010, http://cyber.law.harvard.edu/publications/2010/DDoS_Independent_Media_Human_Rights.

[34] En mars 2013, par exemple, le *Los Angeles Times* a publié un rectificatif après avoir affirmé que ce dont Anonymous avait été accusé pouvait être assimilé à du piratage. Voir Matt Pearce, «Wisconsin Man Indicted in Anonymous Attack of Koch Industries», *The Los Angeles Times*, 27 mars 2013. Le rectificatif se trouve vers la fin de l'article.

[35] Lee Mathews, «Man Fined $183,000 for Helping Anonymous DDoS a Site for One Minute», *Geek*, 10 décembre 2013, www.geek.com/apps/man-fined-183000-for-helping-anonymous-ddos-a-site-for-one-minute-1579317; Ryan J. Reilly, «Loading Koch Industries Site Too Many Times in 1 Minute Just Cost this Truck Driver $183,000», *Huffington Post*, 3 décembre 2013, www.huffingtonpost.com/2013/12/02/anonymous-koch-attack_n_4374365.html.

[36] Sandra Laville, «Student Convicted over Anonymous Cyber-Attacks», *The Guardian*, 6 décembre 2012.

[37] Joe Kloc, «Anonymous's PayPal 14 Enter Pleas, Most May Skirt Jail», *The Daily Dot*, 5 décembre 2013, www.dailydot.com/politics/anonymous-paypal-14-pleas-jail-fine.

[38] Anu Passary, «Anonymous Members Plead Guilty in Paypal DDoS Attack Case», *Tech Times*, 8 décembre 2013, www.techtimes.com/articles/1874/20131208/anonymous-members-plead-guilty-in-paypal-ddos-attack-case.htm.

[39] Somini Sengupta, «British Police Make Arrest in Net Attacks», *The New York Times*, 27 juillet 2011.

Notes du chapitre 5

[1] Eduard Kovacs, «Anonymous Hackers Leak Documents on Governor of Italy's Lombardy Region», *Softpedia*, 25 novembre 2013, http://news.softpedia.com/news/Anonymous-Hackers-Leak-Documents-on-Governor-of-Italy-s-Lombardy-Region-403190.shtml.

[2] Voir Carola Frediani, *Inside Anonymous: A Journey into the World of Cyberactivism*, s.l., InformAnt, 2013.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

[3] Lina Ben Mhenni, «Tunisia: Censorship Continues as WikiLeaks Cables Make the Rounds», *Global Voices*, 7 décembre 2010, https://globalvoices.org/2010/12/07/tunisia-censorship-continues-as-wikileaks-cables-make-the-rounds.

[4] Quinn Norton, «2011: The Year Anonymous Took On Cops, Dictators and Existential Dread», *Wired*, 11 janvier 2012, www.wired.com/2012/01/anonymous-dicators-existential-dread.

[5] Ibrahim Saleh, «WikiLeaks and the Arab Spring: The Twists and Turns of Media, Culture, and Power», dans *Beyond WikiLeaks: Implications for the Future of Communications, Journalism and Society*, New York, Palgrave Macmillan, 2013, p. 237.

[6] Câble diplomatique 09TUNIS516-a, traduit et reproduit par la rédaction de Nawaat, «Un dîner avec Sakher El Matri», *Nawaat*, 15 décembre 2010, http://nawaat.org/portail/2010/12/15/tunileaks-tunisie-un-diner-avec-sakhr-el-matri-traduction.

[7] John Pollock, «How Egyptian and Tunisian Youth Hacked the Arab Spring», *MIT Technology Review*, 23 août 2011, www.technologyreview.com/featuredstory/425137/streetbook.

[8] Fœtus, «L'essence de Takriz», *Takriz*, janvier 2010.

[9] «Sidi Bouzid: un enterrement et des tensions», *Jeune Afrique*, 6 janvier 2011.

[10] «Grève massive des avocats en Tunisie», *Libération*, 6 janvier 2011.

[11] Tarek Amara, «Tunisian Government Says Two Killed in Clashes», Reuters, 9 janvier 2011, www.reuters.com/article/2011/01/09/us-tunisia-protests-idUSTRE70809V20110109.

[12] Voir anonnews.org/press/item/135.

[13] Pour des articles représentatifs de la propension des médias à qualifier Sabu de chef, voir: Charles Arthur, «The Darkness at the Heart of Anonymous», *The Guardian*, 23 août 2011; Josh Halliday, «LulzSec Mastermind Sabu: An Elite Hacker and Star FBI Informant», *The Guardian*, 6 mars 2012; Andy Greenberg, «LulzSec Leader and Informant "Sabu" Let Off with Time Served», *Wired*, 27 mai 2014, www.wired.com/2014/05/hector-monsegur-sabu-sentencing. Pour des articles où l'on affirme que le chef est plutôt Topiary, voir: Adrian Chen, «Meet the LulzSec Leader Arrested by British Police Today», *Gawker*, 27 juillet 2011, http://gawker.com/5825248/meet-the-lulzsec-leader-arrested-by-british-police-today; Peter Finocchiaro, «LulzSec Leader "Topiary" Arrested in Britain», *Salon*, 27 juillet 2011, www.salon.com/2011/07/27/lulzsec_topiary_arrest.

[14] John Cook et Adrian Chen, «Inside Anonymous' Secret War Room», *Gawker*, 18 mars 2011, http://gawker.com/5783173/inside-anonymous-secret-war-room.

[15] Arthur, «The Darkness at the Heart of Anonymous», *loc. cit.*

[16] Joseph Menn, «SPECIAL REPORT—U.S. Cyberwar Strategy Stokes Fear of Blowback», *Reuters*, 10 mai 2013, www.reuters.com/article/2013/05/10/us-usa-cyber weapons-specialreport-idUSBRE9490EL20130510.

[17] *Ibid.*

[18] Bien que j'aie eu accès à la plupart des fichiers journaux ultérieurs, on n'y trouve aucune mention des raisons pour lesquelles l'attaque jour zéro ne s'est pas concrétisée. Aucun des participants auxquels j'ai posé la question ne se rappelait pourquoi. Il n'est pas rare qu'une action débattue et envisagée finisse par ne pas avoir lieu et sombrer dans l'oubli.

[19] Tom Jagatic *et al.*, «Social Phishing», *Communications of the ACM*, automne 2007, p. 94-100.

[20] «St. Jude Memorial and Virtual Wake», *The Well*, 1er août 2003, www.well.com/conf/inkwell.vue/topics/190/St-Jude-Memorial-and-Virtual-Wak-page01.html.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

[21] Spencer Ackerman, «Former NSA Chief Warns of Cyber-Terror Attacks if Snowden Apprehended», *The Guardian*, 6 août 2013.

[22] Ryan J. Reily, «Stephen Heymann, Aaron Swartz Prosecutor, Compared Internet Activist to Rapist: MIT Report», *Huffington Post*, 31 juillet 2013, www.huffingtonpost.com/2013/07/31/stephen-heymann-aaron-swartz_n_3685191.html.

[23] Hal Abelson, «The Lessons of Aaron Swartz», *MIT Technology Review*, 4 octobre 2013, www.technologyreview.com/view/519866/the-lessons-of-aaron-swartz.

[24] Gabriella Coleman, «Gabriella Coleman's Favorite News Stories of the Week», *Techdirt*, 12 octobre 2013, www.techdirt.com/articles/20131011/16530924846/gabriella-colemans-favorite-news-stories-week.shtml.

[25] Miller McPherson, Lynn Smith-Lovin et James M. Cook, «Birds of a Feather: Homophily in Social Networks», *Annual Review of Sociology*, vol. 27, nº 1, 2001, p. 415-444.

[26] Roli Varma, «Why So Few Women Enroll in Computing? Gender and Ethnic Differences in Students' Perception», *Computer Science Education*, vol. 20, nº 4, 2010, p. 301-316.

[27] Pour des données plus précises, voir Christina Dunbar Hester et Gabriella Coleman, «Engendering Change? Gender Advocacy in Open Source», *Culture Digitally*, 26 juin 2012, http://culturedigitally.org/2012/06/engendering-change-gender-advocacy-in-open-source/.

[28] *Ibid.*

[29] Voir Douglas Thomas, *Hacker Culture*, Minneapolis, University of Minnesota Press, 2003.

Notes du chapitre 6

[1] Barret Brown, message Twitter, 9 novembre 2011, 21 h 56, https://twitter.com/BarrettBrownLOL/status/134464512064626689.

[2] Barret Brown, «Why the Hacks Hate Michael Hastings», *Vanity Fair*, 23 juin 2010, www.vanityfair.com/news/2010/06/why-the-hacks-hate-michael-hastings.

[3] Ian Shapira, «"Anonymous" Movement Views Web Hijinks as Public Good, but Legality Is Opaque», *The Washington Post*, 25 janvier 2011.

[4] Richard Borshay Lee, «Eating Christmas in the Kalahari», *Natural History*, décembre 1969.

[5] Hillary Clinton, citée dans Merle David Kellerhals Jr, «Manifestations égyptiennes: les É.-U. appellent à la retenue», *IIP Digital*, Bureau des programmes d'information internationale du département d'État des États-Unis, 27 janvier 2011.

[6] Bien que certains y aient trempé, les Anons ne pratiquent pas la fraude de cartes bancaires ou le vol d'identité à grande échelle. En novembre 2006, un des réseaux de fraudeurs les plus notoires, Shadowcrew, s'est fait pincer lors de ce que le journaliste Kevin Poulsen a qualifié de «plus important coup de filet de l'histoire des États-Unis contre des voleurs d'identité». Kevin Poulsen, *Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground*, New York, Broadway, 2011, p. 113.

[7] Pour le meilleur compte rendu de l'opération Sundevil, voir Bruce Sterling, *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, New York, Bantam, 1992, www.mit.edu/hacker/hacker.html.

[8] «Document Management in the FBI», chap. 2 de *An Investigation of the Belated Production of Documents in the Oklahoma City Bombing Case*, Département américain de la Justice, 19 mars 2002,

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

www.justice.gov/oig/special/0203/chapter2.htm.

[9] Parce qu'il ne consiste qu'en un résumé, et non en une transcription intégrale, le document *FD-302* est depuis longtemps critiqué par les militants et les juristes pour ses aprioris ou ses partis pris. L'avocat spécialisé dans les droits de la personne Harvey Silverglate a synthétisé ses lacunes dans une lettre d'opinion: «Effrayée, désorientée, une personne interrogée qui nie le moindre propos que lui attribue un *FD-302* pourrait être accusée de fausse déclaration.» (Harvey Silvergate, «Unrecorded Testimony», *The Boston Globe*, 11 mai 2013.) En mai 2014, le FBI a révisé sa politique: un enregistrement est désormais requis dans la plupart des interrogatoires de suspects de juridiction fédérale. (Andrew Grossman, «FBI to Record Most Interrogations of Suspects in Federal Custody», *The Wall Street Journal*, 21 mai 2014.)

Notes du chapitre 7

[1] J. Edgar Hoover, *Counterintelligence Program, Black Nationalist—Hate Groups Racial Intelligence*, note de service, 4 mars 1968, cité dans Jules Boykoff, *The Suppression of Dissent: How the State and Mass Media Squelch USAmerican Social Movements*, New York, Routledge, 2006, p. 121.

[2] Boykoff, *op. cit.*, p. 115-117.

[3] FBI (anonyme), lettre à Martin Luther King, citée dans *ibid.*, p. 118.

[4] US Senate Committee to Study Governmental Operations with Respect to Intelligence Activities, «COINTELPRO: The FBI's Covert Action Programs Against American Citizens», 23 avril 1976, http://terrasol.home.igc.org/HooverPlan.htm.

[5] Cité dans «The FBI, COINTELPRO and the Most Important Robbery You've Never Heard Of», *Privacy SOS*, 3 avril 2013, www.privacysos.org/node/1015.

[6] Mark Mazzetti, «Burglars Who Took on F.B.I. Abandon Shadows», *The New York Times*, 7 janvier 2014.

[7] Glenn Greenwald, «The Leaked Campaign to Attack Wikileaks and Its Supporters», *Salon*, 11 février 2011, www.salon.com/2011/02/11/campaigns_4.

[8] Nelson D. Schwartz, «Facing Threat from WikiLeaks, Bank Plays Defense», *The New York Times*, 2 janvier 2011.

[9] Voir Eric Lipton et Charlie Savage, «Hackers Reveal Offers to Spy on Corporate Rivals», *The New York Times*, 11 février 2011.

[10] Marcus Kabel, «Ark. Court Says Wal-Mart Can Copy Data of Fired Worker», *The San Diego Union-Tribune*, 13 avril 2007.

[11] Gary Ruskin, «Spooky Business: Corporate Espionage Against Nonprofit Organizations», Center for Corporate Policy, 20 novembre 2013, www.corporatepolicy.org/spookybusiness.pdf.

[12] *Ibid.* C'est moi qui souligne.

[13] Peter Bright, Nate Anderson et Jacqui Chang, *Unmasked*, Amazon Digital Services, 2011, p. 54.

[14] Nicole Perlroth et David E. Sanger, «Nations Buying as Hackers Sell Flaws in Computer Code», *The New York Times*, 13 juillet 2013.

[15] Ryan Gallagher, «Cyberwar's Gray Market», *Slate*, 16 janvier 2013, www.slate.com/articles/technology/future_tense/2013/01/zero_day_exploits_should_the_hacker_gray_market_be_regulated.html.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

[16] Nate Anderson, «Black Ops: How HBGary Wrote Backdoors for the Government», *Ars Technica*, 21 février 2011, http://arstechnica.com/tech-policy/2011/02/black-ops-how-hbgary-wrote-backdoors-and-rootkits-for-the-government.

[17] Ruskin, «Spooky Business», *loc. cit.*, p. 3.

[18] Voir http://pastebin.com/raw.php?i=u4mtivNN.

[19] Mike Masnick, «Play by Play of How HBGary Federal Tried to Expose Anonymous... and Got Hacked Instead», *Techdirt*, 11 février 2011, www.techdirt.com/articles/20110211/11013413056/play-play-how-hbgary-federal-tried-to-expose-anonymous-got-hacked-instead.shtml; Nate Anderson, «How One Man Tracked Down Anonymous—And Paid a Heavy Price», *Wired*, 10 février 2011, www.wired.com/2011/02/anonymous.

[20] Joseph Menn, «Cyberactivists Warned of Arrest», *Financial Times*, 5 février 2011.

[21] Dans des courriels échangés à l'automne 2010, on envisageait la fermeture de HBGary Federal pour cause de rentabilité insuffisante, et on affirmait que «le poste de PDG d'Aaron Barr [était] en jeu». (Voir page 28 de Bright, Anderson et Chang, *Unmasked*, *op. cit.*, pour les courriels faisant état de la situation financière de l'entreprise.)

[22] Peter Bright, «Anonymous Speaks: The Inside Story of the HBGary Hack», *Ars Technica*, 15 février 2011, http://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack.

[23] Fragment de Karl Wilhelm Friedrich von Schlegel, philosophe romantique du XIXe siècle (et grand marginal). Friedrich von Schlegel, *Fragments*, Paris, José Corti, 1996, p. 134.

[24] Voir http://archive.today/lMuqh#selection-207.17-207.32.

[25] John Cook et Adrian Chen, «Inside Anonymous' Secret War Room», *Gawker*, 18 mars 2011, http://gawker.com/5783173/inside-anonymous-secret-war-room.

[26] Dan Kaplan, «Anonymous Takes Over Security Firm in Vengeful Hack», *SC Magazine*, 7 février 2011, www.scmagazine.com/anonymous-takes-over-security-firm-in-vengeful-hack/article/195837.

[27] «Hacker of Sacramento Company HBGary Pleads Guilty», communiqué de presss du FBI, 6 mars 2012, www.fbi.gov/sacramento/press-releases/2012/hacker-of-sacramento-company-hbgary-pleads-guilty.

[28] Parmy Olson, «Victim of Anonymous Attack Speaks Out», *Forbes*, février 2011.

[29] Selon le plan, Palantir aurait fourni un coûteux logiciel d'analyse de liens opérant à partir d'un serveur, tandis que Berico aurait préparé le contrat précisant le mode de gestion du projet et le développement des ressources, de la méthodologie et des processus à élaborer. HBGary Federal aurait collaboré en fournissant des «renseignements numériques» et «en exploitant les médias sociaux». Nate Anderson, «Spy Games: Inside the Convoluted Plot to Bring Down WikiLeaks», *Ars Technica*, 14 février 2011, http://arstechnica.com/tech-policy/2011/02/the-ridiculous-plan-to-attack-wikileaks.

[30] Parmy Olson, «Congressman Probing HBGary Scandal Fears "Domestic Surveillance"», *Forbes*, 23 mars 2011, www.forbes.com/sites/parmyolson/2011/03/23/congressman-probing-hbgary-scandal-fears-domestic-surveillance.

[31] Barrett Brown, «The Cyber-Intelligence Complex and Its Useful Idiots», *The Guardian*, 1er juillet 2013.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

[32] Tim Shorrock, «US Intelligence & Oursourcing», http://timshorrock.com/?page_id=141.

[33] Tim Shorrock, «Put the Spies Back Under One Roof», *The New York Times*, 17 juin 2013.

Notes du chapitre 8

[1] Steve Ragan, collaborateur au *Tech Herald*, a aussi communiqué avec des membres de LulzSec dans le cadre d'un reportage sur les aspects techniques du piratage.

[2] David Mirza, entretien avec l'auteure.

[3] 2600, message Twitter, 22 juillet 2013, 10 h 22, http://twitter.com/2600/status/76931363755925504.

[4] «Anonymous Vs. Crito: FAQ and questions for Anons», Asherah Research Group, 24 mai 2012, www.asherahresearch.net/?page_id=416.

[5] «Anonymous Message to Sony about Taking Down Playstation Network», vidéo YouTube, publiée par Johnny John, 22 avril 2011, www.youtube.com/watch?v=aTbLA_1nkgU.

[6] «The Light It Up Contest—Geohot», vidéo YouTube, publiée par geohot, 12 février 2011, www.youtube.com/watch?v=9iUvuaChDEg.

[7] Cory Doctorow, «Embattled PS3 Hacker Raises Big Bank to Fight Sony», *Boing Boing*, 22 février 2011, http://boingboing.net/2011/02/22/embattled-ps3-hacker.html.

[8] Cité dans Jason Mick, «Anonymous Engages in Sony DDoS Attacks over GeoHot PS3 Lawsuit», *DailyTech*, 4 avril 2011, www.dailytech.com/Anonymous+Engages+in+Sony+DDoS+Attacks+Over+GeoHot+PS3+Lawsuit/article21282.htm.

[9] Patrick Seybold, «Update on PlayStation Network and Qriocity», *PlayStation.Blog*, 26 avril 2011, http://blog.us.playstation.com/2011/04/26/update-on-playstation-network-and-qriocity.

[10] Colin Milburn, «Long Live Play: The PlayStation Network and Technogenic Life», dans Bernadette Bensaude-Vincent *et al.* (dir.), *Attractive Objects: The Furniture of the Technoscientific World*, Pittsburgh, University of Pittsburgh Press, à paraître.

[11] Owen Good, «Welcome Back PSN: The Winners», *Kotaku*, 21 mai 2011, http://kotaku.com/5804318/welcome-back-psn-the-winners.

[12] Paul Tassi, «Sony Pegs PSN Attack Costs at $170 Million, $3.1B Total Loss for 2011», *Forbes*, 23 mai 2011, www.forbes.com/sites/insertcoin/2011/05/23/sony-pegs-psn-attack-costs-at-170-million.

[13] «Sony Fined £250,000 After Millions of UK Gamers' Details Compromised», Information Commissioner's Office, 24 janvier 2013, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2013/01/sony-fined-250-000-after-millions-of-uk-gamers-details-compromised/.

[14] Se prononce «*Lulz for your security*», ce qui signifie «le *lulz* pour votre sécurité». [NdT]

[15] «Outro», *HTP Zine 5*, 2013, www.exploit-db.com/papers/25306.

[16] LulzSec, message Twitter, 10 mai 2011, 7 h 52, http://twitter.com/LulzSec/status/68116303004708864.

[17] Photo: Alexander Sotirov. Reproduite avec l'autorisation de son auteur.

[18] Pour un excellent tour d'horizon des nombreuses menaces à la sécurité d'internet, voir Ron Deibert, *Black Code: Surveillance, Privacy, and the Dark Side of the Internet*, Toronto, Signal, 2013.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

[19] «Hackers Testifying at the United States Senate, May 19, 1998 (L0pht Heavy Industries)», vidéo YouTube, publiée par Joe Grand, 14 mars 2011, www.youtube.com/watch?v=VVJldn_MmMY.

[20] En fait, selon un rapport sur la sécurité d'internet, le nombre d'infiltrations a augmenté de 30 % en 2013 par rapport à 2012. Ces données ne sont pas nécessairement exhaustives, mais elles donnent une idée du nombre d'infiltrations survenues au cours d'une année en particulier. Voir «ITRC 2013 Breach List Tops 600 in 2013», Identity Theft Resource Center, 20 février 2014, www.idtheftcenter.org/ITRC-Surveys-Studies/2013-data-breaches.html.

[21] Patrick Gray, «Why We Secretly Love LulzSec», *Risky Business*, 8 juin 2011, http://risky.biz/lulzsec.

[22] Michael Taussig, *Defacement: Public Secrecy and the Labor of the Negative*, Stanford (CA), Stanford University Press, 1999, p. 5.

[23] Voir la page d'accueil de TTI/Vanguard: www.ttivanguard.com.

[24] Dick Hebdige, *Sous-culture. Le sens du style*, Paris, Zones, 2008 [c1979].

[25] Un important producteur hollywoodien vient d'acheter les droits d'adaptation cinématographique d'un article du magazine *Rolling Stone* sur l'opération Steubenville, une opération d'Anonymous relative à une affaire de viol survenue en Ohio. Tant que le film ne sera pas sorti, on ne saura pas s'il déforme et affadit le message contre-culturel de l'organisation.

[26] Friedrich Nietzsche, *Ainsi parlait Zarathoustra*, Paris, GF-Flammarion, 2006, p. 52.

[27] Pour un exposé en profondeur sur le rôle de l'esthétique et de l'hyperbole dans la pensée et les écrits de Nietzsche, voir Alexander Nehamas, *Nietzsche. La vie comme littérature*, Paris, Presses universitaires de France, 1994.

[28] Nietzsche, *Ainsi parlait Zarathoustra*, *op. cit.*, p. 80.

[29] *Ibid.*, p. 158.

[30] Walter Benjamin, *Critique de la violence*, Paris, Petite Bibliothèque Payot, 2012, p. 63.

Notes du chapitre 9

[1] Chris Hedges, «The Revolutionaries in Our Midst», *Truthdig*, 10 novembre 2013, www.truthdig.com/report/item/the_revolutionaries_in_our_midst_20131110.

[2] Bruce Sterling, *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, New York, Bantam, 1992, www.mit.edu/hacker/hacker.html.

[3] *Ibid.* Cette liste de *philes* ne représente qu'une fraction de ceux qu'énumère l'ouvrage de Sterling.

[4] Hacktivists of the world, unite, «Philippine Hackers Target National Police, Demanding the Release of the Sagada 11!», *Indybay*, 22 mars 2006, www.indybay.org/newsitems/2006/03/22/18099531.php. Voir aussi «Electronic Civil Disobedience Journal», *Hack This Site*, 2007, http://mirror.hackthissite.org/hackthiszine/hackthiszine5.txt

[5] Stuart Luman, «The Hacktivist», *Chicago Magazine*, 25 juin 2007, www.chicagomag.com/Chicago-Magazine/July-2007/The-Hacktivist.

[6] «Operation Anti-Security», *Pastebin*, 19 juin 2011, http://pastebin.com/9KyA0E5v.

[7] «Intro», *antiSecurity*, http://web.archive.org/20010301215117/http://anti.security.is.

[8] The Lulz Boat, message Twitter, 4 juin 2011, 5 h 34, http://twitter.com/LulzSec/status/76960035145650177.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

[9] Stephen Chapman, «Operation Anti-Security: LulzSec and Anonymous Target Banks and Governments», *ZDNet*, 20 juin 2011, www.zdnet.com/article/operation-anti-security-lulzsec-and-anonymous-target-banks-and-governments.

[10] «Chinga La Migra Bulletin #1», 23 juin 2011, http://thepiratebay.se/torrent/6490796/Chinga_La_Migra.

[11] «50 Days of Lulz», *Pastebin*, 25 juin 2011, http://pastebin.com/1znEGmHa.

[12] Samantha Murphy, «Exclusive First Interview with Key LulzSec Hacker», *New Scientist*, nº 2820, 9 juillet 2011; accessible en ligne: www.newscientist.com/article/dn20649-exclusive-first-interview-with-key-lulzsec-hacker#.6bPdB_7Gi0.

[13] Aldous Huxley, *Des Caraïbes au Mexique. Journal d'un voyageur*, Paris, La Table ronde, 1992, p. 126.

[14] Topiary, message Twitter, 21 juillet 2011, 21 h 02, https://twitter.com/atopiary/status/94225773896015872.

[15] Trouble de stress post-traumatique. [NdT]

[16] Mark Schone (dir.), «Exclusive: Snowden Docs Show UK Spies Attacked Anonymous, Hackers», *NBC News*, 4 février 2014, www.nbcnews.com/news/investigations/war-anonymous-british-spies-attacked-hackers-snowden-docs-show-n21361.

[17] Chris Weatherhead, message Twitter, 5 février 2014, 8 h 39, http://twitter.com/CJFWeatherhead/status/431059633071878144.

[18] Transcript, *CNN Newsroom*, 15 août 2011, http://quiz.cnn.com/TRANSCRIPTS/1108/15/cnr.08.html.

[19] See Paolo Gerbaudo, *Tweets and the Streets: Social Media and Contemporary Activism*, Londres, Pluto, 2012.

[20] «Disguised Member of Hacktivist Group "Anonymous" Defends Retaliatory Action Against BART», *Democracy Now!*, 16 août 2011, www.democracynow.org/2011/8/16/disguised_member_of_hacktivist_group_anonymous.

[21] «Untitled», *Pasetbin*, 19 août 2011, http://pastebin.com/zug52JVA.

[22] «Anonymous Is Not Unanimous», *Pastebin*, 17 août 2011, http://pastebin.com/4vprKdXH.

[23] Voir Chantal Mouffe, «Deliberative Democracy or Agonistic Pluralism?», *Social Research*, vol. 66, nº 3, automne 1999, p. 745-758.

Notes du chapitre 10

[1] The Real Sabu, message Twitter, 17 août 2011, 4 h 43, http://twitter.com/anonymouSabu/status/103763961064865792.

[2] The Real Sabu, message Twitter, 17 septembre 2011, 13 h 43, http://twitter.com/anonymousabu/status/115133670213435393.

[3] The Real Sabu, message Twitter, 17 septembre 2011, 13 h 52, http://twitter.com/anonymouSabu/status/115136117925347328.

[4] «USA v. Hector "Sabu" Monsegur Transcript August 15, 2011», *Cryptome*, http://cryptome.org/2013/02/usa-v-monsegur-11-0815.htm.

[5] Voir http://pastie.org/private/om3mrqvbdbmg8esddkcmw#2-3,347,353,365,376.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

[6] Nathan Schneider, *Thank You, Anarchy: Notes from the Occupy Apocalypse*, Berkeley, University of California Press, 2013, p. 28.

[7] Église épiscopalienne de Manhattan située près du parc Zuccotti. L'Église appuie le mouvement Occupy Wall Street à ses débuts, mais prend ses distances lorsque les manifestants envisagent d'établir un campement sur son terrain. [NdT]

[8] Drew Grant, «Hacker Hero "Weev" Stops by Occupy Wall Street» (vidéo), *Observer*, 21 octobre 2011, http://observer.com/2011/10/hacker-hero-weev-stops-by-occupy-wall-street-video.

[9] Graham Jones, *Tricks of the Trade: Inside the Magician's Craft*, Berkeley, University of California Press, 2011, p. 94.

[10] Jeanne Mansfield, «Why I Was Maced at the Wall Street Protests», *Pastebin*, 26 septembre 2011, http://pastebin.com/Wkckd9bR.

[11] «BadCopd0x», *Pastebin*, 26 septembre 2011, http://pastebin.com/nC4f5uca.

[12] «Anthony Bologna, Pepper Spray NYPD Officer, Transferred to Work in Staten Island», *Huffington Post*, 26 octobre 2011, www.huffingtonpost.com/2011/10/26/anthony-bologna-nypd-offi_n_1033382.html.

[13] Karen McVeigh, «Occupy Wall Street: "Pepper-Spray" Officer Named in Bush Protest Claim», *The Guardian*, 27 septembre 2011.

[14] City of New York, Information Technology & Telecommunications, «DoITT—Frequently Asked Questions—Public Pay Telephones», www.nyc.gov/html/doitt/html/faq/payphone.shtml.

[15] «Sabu / LulzSec leader», *Pastebin*, 7 juin 2011, http://pastebin.com/TVnGwSmG. Certains détails de cet épisode sont tirés du fascinant portrait de Sabu rédigé par Steve Fishman: «"Hello, I Am Sabu..."», *New York Magazine*, 3 juin 2012, http://nymag.com/news/features/lulzsec-sabu-2012-6.

[16] Pour une réflexion critique approfondie sur les rapports de genres dans la communauté geek, voir Geekfeminism.org.

[17] Dans un article, Meredith Patterson se penche sur le rôle de l'excentricité: Meredith Patterson, «When Nerds Collide», *Medium*, 23 mars 2014, https://medium.com/@maradydd/when-nerds-collide-31895b01e68c#.ph57mzfe8.

[18] Junot Díaz, *La brève et merveilleuse vie d'Oscar Wao*, Paris, Plon, coll. «Feux croisés», 2009, p. 17.

[19] Quinn Norton, «How Antisec Died», *Medium*, 21 novembre 2013, https://medium.com/quinn-norton/how-antisec-died-654abf6aeff7#.r3v6h2gqh.

[20] Schneider, *Thank You, Anarchy*, *op. cit.*, p. 76.

[21] *Fusion centers*. Centres chargés de faire circuler l'information entre agences de renseignement, police fédérale, forces armées, départements fédéraux et gouvernements locaux. [NdT]

[22] «FBI Documents Reveal Secret Nationwide Occupy Monitoring», Partnership for Civil Justice Fund, 22 décembre 2012, www.justiceonline.org/commentary/fbi-files-ows.html.

[23] Colin Moynihan, «Officials Cast Wide Net in Monitoring Occupy Protests», *The New York Times*, 23 mai 2014.

[24] David Hume, *Traité de la nature humaine*, livre II, *Dissertations sur les passions*, Paris, GF-Flammarion, 1991, p. 155.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Notes du chapitre 11

[1] «Operation m4yh3m», http://ulrikbrask.dk/operation-m4yh3m.

[2] *Ibid.*

[3] The Real Sabu, message Twitter, 24 décembre 2011, 14 h 49, http://twitter.com/anonymouSabu/status/150664330763964416.

[4] Comité invisible, *L'insurrection qui vient*, Paris, La Fabrique, 2007, p. 100.

[5] «Operation m4yh3m», *loc. cit.*

[6] The Real Sabu, message Twitter, 25 décembre 2011, 15 h 54, http://twitter.com/anonymouSabu/status/151043065501593601.

[7] *Ibid.*, 25 décembre 2011, 16 h 57, http://twitter.com/anonymouSabu/status/151059108353683456.

[8] «Press Release: The Stratfor Hack is not the Work of Anonymous», *Pastebin*, 25 décembre 2011, http://pastebin.com/8yrwyNkt.

[9] Malcolm Gladwell, *Les prodiges. Pourquoi les qualités personnelles et le talent ne suffisent pas à expliquer le succès*, Montréal, Transcontinental, 2009.

[10] Kevin Poulsen, «WikiLeaks Volunteer Was a Paid Informant for the FBI», *Wired*, 27 juin 2013, www.wired.com/2013/06/wikileaks-mole.

[11] Pour la liste complète des sites participants, voir SopaStrike.com.

[12] Chenda Ngak, «SOPA and PIPA Internet Blackout Aftermath, Staggering Numbers», *CBS News*, 19 décembre 2012, www.cbsnews.com/news/sopa-and-pipa-internet-blackout-aftermath-staggering-numbers.

[13] Victoria Espinel, Aneesh Chopra et Howard Schmidt, «Combating Online Piracy While Protecting an Open and Innovative Internet», *We the People: Your Voice in Our Government*, http://petitions.whitehouse.gov/response/combating-online-piracy-while-protecting-open-and-innovative-internet.

[14] Greg Sandoval, «New Zealand PM Apologizes to Kim Dotcom; Case Unraveling», *CNET*, 27 septembre 2012, www.cnet.com/news/new-zealand-pm-apologizes-to-kim-dotcom-case-unraveling.

[15] Max Fisher, «Stratfor Is a Joke and So Is Wikileaks for Taking It Seriously», *The Atlantic*, 27 février 2012, www.theatlantic.com/international/archive/2012/02/stratfor-is-a-joke-and-so-is-wikileaks-for-taking-it-seriously/253681.

[16] «Re: Wiki Hackers Talk to *The Economist*», *The Global Intelligence Files*, 28 mars 2013, http://wikileaks.org/gifiles/docs/10/1075390_re-wiki-hackers-talk-to-the-economist-.html.

[17] Steve Horn, «How to Win the Media War Against Grassroots Activists: Stratfor's Strategies», *MintPress News*, 29 juillet 2013, www.mintpressnews.com/stratfor-strategies-how-to-win-the-media-war-against-grassroots-activists/166078.

[18] Entretien par courriel avec l'auteure.

[19] Scott Stewart, «Re: [alpha] INSIGHT-US-Occupy Austin and Deep Green Resistance-NO CODE», courriel cité dans Gary Ruskin, «Spooky Business: Corporate Espionage Against Nonprofit Organizations», Center for Corporate Policy, 20 novembre 2013, www.corporatepolicy.org/spookybusiness.pdf.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

[20] «Stratfor Statement on Wikileaks», *Digital Journal*, 27 février 2012, www.digitaljournal.com/pr/599356.

[21] The Real Sabu, message Twitter, 3 février 2012, 22 h 22, http://twitter.com/anonymouSabu/status/165636278770077697.

[22] Jana Winter, «EXCLUSIVE: Inside LulzSec, a Mastermind Turns on His Minions», *Fox News*, 6 mars 2012, www.foxnews.com/tech/2012/03/06/exclusive-inside-lulzsec-mastermind-turns-on-his-minions.html.

[23] The Real Sabu, message Twitter, 16 août 2011, 8 h 22, http://twitter.com/anonymousabu/status/103456479964700672.

[24] Nigel Parry, «Sacrificing Stratfor: How the FBI Waited Three Weeks to Close the Stable Door», *nigelparry.com*, 25 mars 2012, www.nigelparry.com/news/sacrificing-stratfor.shtml.

[25] Winter, «EXCLUSIVE: Inside LulzSec», *loc. cit.*

[26] George Friedman, «The Hack on Stratfor», *Stratfor*, 11 janvier 2012, www.stratfor.com/weekly/hack-stratfor.

[27] Nicole Perlroth, «Inside the Stratfor Attack», *The New York Times*, 12 mars 2012.

[28] Dell Cameron, «How an FBI Informant Orchestrated the Stratfor Hack», *The Daily Dot*, 5 juin 2014, www.dailydot.com/politics/hammond-sabu-fbi-stratfor-hack.

[29] «Sentenced to 10 Years in Prison, Jeremy Hammond Uses Allocution to Give Consequential Statement Highlighting Global Criminal Exploits by FBI Handlers», *The Sparrow Project*, 15 novembre 2013, www.sparrowmedia.net/2013/11/jeremy-hammond-sentence.

[30] Mark Mazzetti, «F.B.I. Informant Is Tied to Cyberattacks Abroad», *The New York Times*, 23 avril 2014.

[31] Daniel Stuckey et Andrew Blake, «Exclusive: How FBI Informant Sabu Helped Anonymous Hack Brazil», *Motherboard*, 5 juin 2014, http://motherboard.vice.com/read/exclusive-how-an-fbi-informant-helped-anonymous-hack-brazil.

[32] Alexandra Natapoff, *Snitching: Criminal Informants and the Erosion of American Justice*, New York, New York University Press, 2011, p. 44.

[33] Lee Romney, «Pressured to Name Names», *Los Angeles Times*, 7 août 2006.

[34] Adam Goldman, «Lawsuit Alleges FBI Is Using No-Fly List to Force Muslims to Become Informants», *The Washington Post*, 22 avril 2014.

[35] «Notes on Sabu Arrest», Errata Security, 6 mars 2013, http://blog.erratasec.com/2012/03/notes-on-sabu-arrest.html#.U64Kjx_7Gb8.

[36] Parmy Olson, *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous and the Global Cyber Insurgency*, New York, Back Bay, 2013, p. 400.

[37] John Leyden, «Sabu Wasn't the Only FBI Mole in LulzSec, Suggest Leaked Docs», *The Register*, 10 janvier 2014, www.theregister.co.uk/2014/01/10/lulzsec_warrants_leak.

[38] Ruth Rosen, *The World Split Open: How the Modern Women's Movement Changed America*, 2e éd., New York, Penguin, 2006, p. 81.

[39] Brian Todd et Kevin Bohn, «Computers of Obama, McCain Campaigns Hacked», *The Political Ticker*, 6 novembre 2008, http://politicalticker.blogs.cnn.com/2008/11/06/computers-of-obama-mccain-campaigns-hacked.

[40] Entretien en ligne avec l'auteure.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

[41] «La Commission des droits de la personne condamne la loi 78», *ICI Radio-Canada*, 19 juillet 2012, www.radio-canada.ca/nouvelles/Politique/2012/07/19/002-loi-speciale-commission.shtml; «Quebec Human Rights Commission Slams Bill 78», *CBC News*, 19 juillet 2012, www.cbc.ca/news/canada/montreal/quebec-human-rights-commission-slams-bill-78-1.1191057.

[42] AnonOpsIndia, message Twitter, 17 mai 2012, 6 h 08, http://twitter.com/opindia_revenge/status/203079500983050240.

[43] «Official Statement from Family and Partner of Aaron Swartz», Remember Aaron Swartz, 12 janvier 2013, http://rememberaaronsw.com/memories.

[44] «Anonymous Operation Last Resort», vidéo YouTube, publiée par Aarons ArkAngel, 26 janvier 2013, www.youtube.com/watch?v=WaPni5O2YyI&feature=youtu.be.

[45] Jason Howerton, «Disturbing Video Leaked of Ohio High School Students Joking About Alleged Gang Rape», *The Blaze*, 2 janvier 2013, www.theblaze.com/stories/2013/01/02/video-of-steubenville-high-school-students-joking-about-alleged-gang-rape-leaked-by-hacktivist-group.

[46] David Kushner, «Anonymous vs. Steubenville», *Rolling Stone*, 27 novembre 2013, www.rollingstone.com/culture/news/anonymous-vs-steubenville-20131127.

[47] Trip Gabriel, «Inquiry in Cover-Up of Ohio Rape Yields Indictment of Four Adults», *The New York Times*, 25 novembre 2013.

[48] «#OpJustice4Rehtaeh», vidéo YouTube, publiée par Anonymous Canada, www.youtube.com/watch?v=7_D_zvizzKA.

[49] Cited in Emily Bazelon, «Non-Consensual Sexting Leads to Child Pornography Charges for Two Men in Rehtaeh Parsons Case», *Salon*, 8 août 2013, www.slate.com/blogs/xx_factor/2013/08/08/rehtaeh_parsons_case_two_years_after_the_initial_report_halifax_police_have.html.

[50] *Ibid.*

[51] «Affaire Rehtaeh Parsons: un an de probation pour un accusé», *La Presse*, 15 janvier 2015.

[52] Peggy Lowe et Monica Sandreczki, «Why Was the Maryville Rape Case Dropped?» *KCUR*, 11 juillet 2013, http://kcur.org/post/why-was-maryville-rape-case-dropped#stream/0.

[53] Ariel Levy, «Trial by Twitter», *The New Yorker*, 5 août 2013.

[54] «Is Maryville the Next Steubenville?», *Huffington Post*, 16 octobre 2013, http://live.huffingtonpost.com/r/segment/is-maryville-the-next-steubenville/525d71012b8c2a4a3d0000d2.

[55] Emily Bazelon, «The Online Avengers», *The New York Times*, 15 janvier 2014.

[56] Le débat a été déclenché par un article de Larisa Mann sur un sujet connexe. Larisa Mann, «What Can Feminism Learn from New Media?», *Communication and Critical/Cultural Studies*, été 2014, p. 1-5.

[57] Stephen Duncombe, *Dream: Re-imagining Progressive Politics in an Age of Fantasy*, New York, New Press, 2007.

Notes de la conclusion

[1] Lauren Cornell, «Primary Documents» (interview de Laura Poitras), *Mousse Magazine*, nº 40, septembre 2013, www.moussemagazine.it/articolo.mm?id=1020.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

[2] Barton Gellman et Julie Tate, «In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are», *The Washington Post*, 5 juillet 2014.

[3] James Risen et Laura Poitras, «N.S.A. Report Outlined Goals for More Power», *The New York Times*, 22 novembre 2013.

[4] Samuel Warren et Louis Brandeis, «The Right to Privacy», *Harvard Law Review*, vol. IV, nº 5, 15 décembre 1890.

[5] Riseup, «Space for Dissent», août 2013, https://help.riseup.net/en/about-us/newsletter/2013/08.

[6] Jennifer Granick, «My Dinner with NSA Director Keith Alexander», *Forbes*, 22 août 2013, www.forbes.com/sites/jennifergranick/2013/08/22/my-dinner-with-general-alexander.

[7] Voir en particulier Will Potter, *Green Is the New Red: An Insider's Account of a Social Movement Under Siege*, San Francisco, City Lights, 2011; et Arun Kundnani, *The Muslims Are Coming!: Islamophobia, Extremism, and the Domestic War on Terror*, New York, Verso, 2014.

[8] Muslim American Civil Liberties Coalition (MACLC), Creating Law Enforcement Accountability & Responsibility (CLEAR) et Asian American Legal Defense and Education Fund (AALDEF), *Mapping Muslims: NYPD Spying and Its Impact on American Muslims*, 2013, http://aaldef.org/Mapping%20Muslims%20NYPD%20Spying%20and%20its%20Impacts%20on%20American%20Muslims.pdf.

[9] Tim Cushing, «Former FBI Agent: NYPD's Muslim-Spying Demographics Unit Was Almost Completely Useless», *Techdirt*, 28 avril 2014, www.techdirt.com/articles/20140423/10254627006/former-fbi-agent-nypds-muslim-spying-demographics-unit-was-almost-completely-useless.shtml.

[10] MACLC, CLEAR et AALDEF, *Mapping Muslims*, *op. cit.*, p. 55.

[11] Glenn Greenwald et Murtaza Hussain, «Under Surveillance», *The Intercept*, 9 juillet 2014, https://theintercept.com/2014/07/09/under-surveillance.

[12] «Factsheet: The NYPD Muslim Surveillance Program», ACLU, www.aclu.org/national-security/factsheet-nypd-muslim-surveillance-program.

[13] Laurie Penny, «If You Live in a Surveillance State for Long Enough, You Create a Censor in Your Head», *New Statesman*, 17 juin 2013, www.newstatesman.com/politics/2013/06/if-you-live-surveillance-state-long-enough-you-create-censor-your-head.

[14] Steve Lohr, «Unblinking Eyes Track Employees», *The New York Times*, 21 juin 2014.

[15] Dernièrement, deux professeurs des universités Northwestern et Princeton ont analysé près de 2 000 nouvelles politiques à la lumière de l'abondance de données disponibles sur les lobbyistes, l'élite américaine et l'opinion des Américains ordinaires. Leur conclusion a confirmé ce que de nombreux observateurs soupçonnaient déjà: «L'élite économique et les organisations représentant les milieux d'affaires ont une influence considérable sur les politiques adoptées aux États-Unis, alors que les groupes qui défendent les intérêts des masses ou des citoyens ordinaires ont peu d'influence.» Martin Gilens et Benjamin Page, «Testing Theories of American Politics: Elites, Interest Groups and Average Citizens», *Perspective on Politics*, vol. 12, nº 3, septembre 2014.

[16] Eben Moglen, «Freedom in the Cloud: Software Freedom, Privacy and Security for Web 2.0 and Cloud Computing», discours prononcé lors d'une réunion de la section new-yorkaise de l'Internet Society, 5 février 2010. Voir www.softwarefreedom.org/events/2010/isoc-ny/FreedomInTheCloud-transcript.html. Bruce Schneier, «The US Government Has Betrayed the Internet. We Need to Take it Back», *The Guardian*, 5 septembre 2013.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

[17] Christopher Soghoian, «Protecting Privacy Can Conflict with Free Business Models», section 7.1 de *The Spies We Trust: Third Party Service Providers and Law Enforcement Surveillance*, thèse de doctorat, université de l'Indiana, août 2012.

[18] Deux ouvrages sur l'engagement politique geek ont été publiés récemment: Jessica L. Bayer, *Expect Us: Online Communities and Political Mobilization*, Oxford, Oxford University Press, 2014; et Patrick Burkhart, *Pirate Politics: The New Information Policy Contests*, Cambridge (MA), MIT Press, 2014.

[19] Trevor Timm, «Congress Wants NSA Reform After All. Obama and the Senate Need to Pass It», *The Guardian*, 20 juin 2014.

[20] Glenn Greenwald, *Nulle part où se cacher*, Paris, J.-C. Lattès, 2014, p. 347.

[21] «La cybersécurité à l'ère post-Snowden», Conférence sur la défense et la sécurité: les théâtres mouvants de l'engagement du Canada, Ottawa, 20 février 2014. Vidéo: www.cpac.ca/fr/programs/dossier-public/episodes/31366144.

[22] Voir le site web Resetthenet.org.

[23] Edward Snowden, cité dans Derek Mead, «"The Bottom Line Is That Encryption Does Work": Edward Snowden at SXSW», *Motherboard*, 10 mars 2014, http://motherboard.vice.com/read/the-bottom-line-is-encryption-does-work-edward-snowden-at-sxsw.

[24] «On the FBI Raid», *Pastebin*, 7 mars 2012, http://pastebin.com/vZEteA3C.

[25] «Why I'm Going to Destroy FBI Agent Robert Smith Part Three Revenge of the Lithe», vidéo YouTube, publiée par Grenalio Kristian Perdana Siahaan, 25 novembre 2012, www.youtube.com/watch?v=VcMHdfvnEk4.

[26] Adrian Chen, «Former Anonymous Spokesman Barrett Brown Indicted for Sharing a Link to Stolen Credit Card Data», *Gawker*, 7 décembre 2012, http://gawker.com/5966757/former-anonymous-spokesman-barrett-brown-indicted-for-sharing-a-link-to-stolen-credit-card-information.

[27] Kevin M. Gallagher, «Barrett Brown, Political Prisoner of the Information Revolution», *The Guardian*, 13 juillet 2013.

[28] Douglas Thomas, *Hacker Culture*, Minneapolis, University of Minnesota Press, 2003, p. 241.

[29] Your Anonymous News, message Twitter, 27 mai 2014, 10 h 53, https://twitter.com/YourAnonNews/status/471318266255011840.

[30] Jeremy Hammond, «Jeremy Hammond Reacts to Hector Monsegur's "Sentencing": Rejects the NSA White Hat Sabu Ideology», *Free Jeremy*, 2 juin 2014, https://freejeremy.net/2014/06/01/jeremy-hammond-reacts-to-hector-monsegurs-sentencing-reject-the-nsa-white-hat-sabu-ideology.

[31] Danilyn Rutherford, «Kinky Empiricism», *Cultural Anthropology*, vol. 27, nº 3, août 2012, p. 465-479.

[32] Anonymous, message Twitter, 12 mai 2014, 11 h 52, http://twitter.com/blackplans/status/465897377468260352.

[33] J'aimerais remercier Scott Kushner d'avoir souligné la différence subtile, mais significative, entre l'absence de volonté de reconnaître une action comme politique et la délégitimation d'une action en raison de son potentiel politique.

[34] Jane Bennett, *The Enchantment of Modern Life: Attachments, Crossings, and Ethics*, Princeton (NJ), Princeton University Press, 2001, p. 4.

[35] Ernst Bloch, *Le principe espérance*, vol. 1, Paris, Gallimard, 1976, p. 9.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

[36] *Ibid.*, p. 12.

[37] Whitney Phillips, *This Is Why We Can't Have Nice Things: Mapping the Relationship Between Online Trolling and Mainstream Culture*, Cambridge (MA), MIT Press, 2015.

[38] David Foster Wallace, «E Unibus Pluram: Television and U.S. Fiction», *Review of Contemporary Fiction*, vol. 13, nº 2, p. 151-194.

[39] «Waiting for the Tsunami Bifo», vidéo YouTube, publiée par alterazionivideo, 29 août 2007, www.youtube.com/watch?v=5eojG4Hom3A&t=10.

[40] Évidemment, vu la pluralité considérable des sociétés industrielles contemporaines, il serait naïf et dangereux de réduire une réalité aussi complexe que les sentiments politiques à de simples «structures de sentiment», pour reprendre le terme commode de Raymond Williams. Il serait tout aussi naïf de rejeter l'ensemble d'une analyse de tendances dominantes (qu'elles soient économiques ou affectives) comme le passage au cynisme. Raymond Williams, *Marxism and Literature*, Oxford, Oxford University Paperback, 1978.

[41] Plan C/The Institute for Precarious Consciousness, «We Are All Very Anxious», *Plan C*, 4 avril 2014, www.weareplanc.org/blog/we-are-all-very-anxious.

[42] Bloch, *Le principe de l'espérance*, *op. cit.*, p. 11.

[43] Richard Sennett, *Ensemble. Pour une éthique de la coopération*, Paris, Albin Michel, 2014, p. 314.

[44] «*We are legion*» renvoie à la réponse qu'un possédé du démon a donnée au Christ: «Légion est mon nom, car nous sommes beaucoup.» (Marc, 5,9). [NdT]

Notes de l'épilogue

[1] Frank Bajak, «Top South American hackers rattle Peru's Cabinet», *CTV News*, 2 septembre 2014, www.ctvnews.ca/sci-tech/top-south-american-hackers-rattle-peru-s-cabinet-1.1986637/comments-7.552819.

[2] Voir le site web de Gamma Group, www.gammagroup.com.

[3] Gamma Group, «Remote Monitoring & Infection Solutions», *The Spy Files*, octobre 2011, https://wikileaks.org/spyfiles/docs/gamma/291_remote-monitoring-and-infection-solutions-finspy-mobile.html.

[4] Morgan Marquis-Boire et Bill Marczak, «From Bahrain With Love: Finfisher's Spy Kit Exposed?», *The Citizen Lab*, 25 juillet 2012, https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed. Même si les chercheurs n'ont pu confirmer que le gouvernement était responsable de l'envoi du logiciel, ils l'ont tout de même laissé entendre en indiquant que les données subtilisées avaient été envoyées à une adresse IP située au Bahreïn. Pour le démenti de Gamma, voir Vernon Silver, «Gamma Says No Spyware Sold to Bahrain; May Be Stolen Copy», *Bloomberg*, 27 juillet 2012, www.bloomberg.com/news/articles/2012-07-27/gamma-says-no-spyware-sold-to-bahrain-may-be-stolen-copy.

[5] Cora Currier et Morgan Marquis-Boire, «Leaked Files: German Spy Company Helped Bahrain Hack Arab Spring Protesters», *The Intercept*, 7 août 2014, https://theintercept.com/2014/08/07/leaked-files-german-spy-company-helped-bahrain-track-arab-spring-protesters.

[6] «Hack Back», s.d., http://0x27.me/HackBack/0x00.txt.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

[7] *Ibid.*

[8] Cora Currier et Morgan Marquis-Boire, «Leaked Documents show FBI, DEA and U.S. Army Buying Italian Spyware», *The Intercept*, 6 juillet 2015, https://theintercept.com/2015/07/06/hacking-team-spyware-fbi.

[9] Hacked Team, message Twitter, 5 juillet 2015, 17 h 26; capture d'écran visible à http://core0.staticworld.net/images/article/2015/07/hackingteam_1-100594937-orig.jpg.

[10] Phineas Fisher, message Twitter, 5 juillet 2015, 23 h 04, https://twitter.com/GammaGroupPR/status/617937092497178624.

[11] Anon2World, message Twitter, 25 juin 2015, 20 h 48, https://twitter.com/Anon2earth/status/614279036278284288.

[12] Steven Chase, «Cyberattack Deals Crippling Blow to Canadian Government Websites», *The Globe and Mail*, 17 juin 2015.

[13] Voir le compte rendu des délibérations du 22 janvier 2015: https://pdf.yt/d/0SWY7AoPOoovRD_a.

[14] *Ibid.*

[15] Quinn Norton, «We Should All Step Back from Security Journalism», *Medium*, 23 janvier 2015, https://medium.com/message/we-should-all-step-back-from-security-journalism-e474cd67e2fa#.l3mtkh2dl.

[16] Voir le site Free Lauri, http://freelauri.com.

[17] ailanthus, «Interview with Tor Summer of Privacy Student Donncha O'Cearbhaill», *Tor*, 3 mai 2015, https://blog.torproject.org/blog/interview-tor-summer-privacy-student-donncha-ocearbhaill.

[18] Voir entre autres Lee Rainie et Mary Madden, *Americans' Privacy Strategies Post-Snowden*, Pew Research Center, 16 mars 2015, www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden.

[19] Nations Unies, Haut-Commissariat aux droits de l'homme, «Le Conseil des droits de l'homme examine des rapports sur la liberté d'opinion et d'expression et sur le droit de réunion et la liberté d'association», communiqué de presse, 17 juin 2015.

[20] James B. Comey, «Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?», allocution prononcée à la Brookings Institution, 16 octobre 2014, www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

[21] Helen Nissenbaum, «The Meaning of Anonymity in an Information Age», *The Information Society*, vol. 15, nº 2, mai 1999, p. 141-144.

[22] Keith Wilson Downey, dans «Our Story», https://thepaypal14.com/story-keth.htm.

[23] Voir https://twitter.com/ro0ted.

[24] Voir le rectificatif qui suit cet article: Matthew Braga, «Anonymous Claims It Leaked Passwords and Credit Card Info of Canadian Officials», *Motherboard*, 23 juin 2015, http://motherboard.vice.com/read/anonymous-claims-it-leaked-passwords-and-credit-card-info-of-canadian-officials.

[25] Peter Sterne, «*Gawker* in the Fight of Its Life With Hulk Hogan Sex-Tape Suit», *POLITICO*, 12 juin 2015, www.capitalnewyork.com/article/media/2015/06/8570075/gawker-fight-its-life-hulk-hogan-sex-tape-suit.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

[26] «Newsweek's Statement on the Bitcoin Story», *Newsweek*, 7 mars 2014.

[27] Bien que rien ne confirme que Nakamoto ait décidé d'intenter des poursuites, des passionnés de Bitcoin ont lancé une campagne de financement participatif pour le soutenir, laquelle a recueilli l'équivalent d'environ 14 000 dollars en bitcoins. Voir «Dorian Nakamoto–Thank You Bitcoin Community», vidéo YouTube publiée par Andreas M. Antonopoulos, 22 avril 2014, www.youtube.com/watch?v=w7YmJZ-qVW8.

[28] Julian Assange, «Assange: How "The Guardian" Milked Edward Snowden's Story», *Newsweek*, 20 avril 2015.

[29] Siobhan Gorman, «Alert on Hacker Power Play», *The Wall Street Journal*, 21 février 2012.

[30] Anonymous (Crypt0nymous), message Twitter, 14 août 2014, 8 h 14, https://twitter.com/Crypt0nymous/status/499937201825001472.

[31] Jack Bratich, «Popular Secrecy and Occultural Studies», *Cultural Studies*, vol. 21, nº 1, janvier 2007, p. 42-58.

[32] Voir aussi Clare Birchall, «Transparency, Interrupted: Secrets of the Left», *Theory, Culture & Society*, vol. 28, nºs 7 et 8, décembre 2011, p. 60-84.

[33] Pour une analyse anthropologique de la logique insidieuse du secret d'État aux États-Unis, voir Joesph Masco, *The Theater of Operations: National Security Affect from the Cold War to the War on Terror*, Durham, Duke University Press, 2014.

[34] Julian Assange (dir.), *Cypherpunks: Freedom and the Future of the Internet*, New York, OR Books, 2012, p. 5.

[35] Voir en particulier Darin Barney, «Publics without Politics: Surplus Publicity as Depoliticization», dans Kirsten Kozolanka (dir.), *Publicity and the Canadian State: Critical Communications Perspectives*, Toronto, University of Toronto Press, 2014, p. 70-86.

[36] Robin Celikates, «Civil Disobedience as a Practice of Civic Freedom», dans David Owen (dir.), *On Global Citizenship: James Tully in Dialogue*, New York, Bloomsbury, 2014, p. 223.

[37] Ewen MacAskill, «Second Leaker in US Intelligence, Says Glenn Greenwald», *The Guardian*, 11 octobre 2014.

[38] Voir Fruzsina Eördögh, «How Big is Anonymous? Maybe Bigger than You Thought», *The Christian Science Monitor*, 8 juillet 2015, www.csmonitor.com/World/Passcode/2015/0708/How-big-is-Anonymous-Maybe-bigger-than-you-thought. Cet article traite d'une étude récente sur la présence d'Anonymous sur Facebook, selon laquelle le collectif de protestataires compte plus de membres et est présent dans un plus grand nombre de pays du monde qu'on le croyait auparavant.

[39] Entretien de l'auteure avec Molly Sauter, 15 juin 2015.

[40] Voir Celia Britton, «Opacity and Transparency: Conceptions of History and Cultural Difference in the Work of Michel Butor and Edouard Glissant», *French Studies*, vol. 49, nº 3, juillet 1995, p. 308-320.

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Table des matières

Avant-propos: Maintenant, vous avez notre attention»

1. Trolls, *tricksters* et *lulz*

2. Opération Chanology: «J'suis venu pour le *lulz*; j'suis resté pour la cause»

3. Les armes des geeks

4. Le coup que le monde entendit

5. *Anonymous Everywhere*

6. Le péril nerd

7. La revanche du *lulz*

8. LulzSec

9. AntiSec

10. Tout secret aspire à être révélé

11. Le sabutage

Conclusion: Aurore

Épilogue: L'état d'Anonymous

Remerciements

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Remarque sur les sources

Glossaire

Notes

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

DÉJÀ PARUS DANS LA COLLECTION «FUTUR PROCHE»

– Normand Baillargeon et Jean-Marc Piotte (dir.), *Au bout de l'impasse, à gauche. Récits de vie militante et perspectives d'avenir*
– Gaétan Breton, *La dette. Règlement de comptes*
– Gaétan Breton, *Faire payer les pauvres. Éléments pour une fiscalité progressiste*
– Gaétan Breton, *Tout doit disparaître. Partenariats public-privé et liquidation des services publics*
– Jean Bricmont, *L'impérialisme humanitaire. Droit humanitaire, droit d'ingérence, doit du plus fort?*
– Noam Chomsky, *Comprendre le pouvoir*
– Noam Chomsky, *Futurs proches. Liberté, indépendance et impérialisme au XXIe siècle*
– Francis Dupuis-Déri (dir.), *Québec en mouvements. Idées et pratiques militantes contemporaines*
– Chris Hedges, *L'empire de l'illusion. La mort de la culture et le triomphe du spectacle*
– Chris Hedges, *La mort de l'élite progressiste*
– Edward S. Herman et David Peterson, *Génocide et propagande. L'instrumentalisation politique des massacres*
– Institut de recherche et d'informations socio-économiques (IRIS), *Dépossession: une histoire économique du Québec contemporain. Tome 1: Les ressources*
– Razmig Keucheyan, *Hémisphère gauche. Une cartographie des nouvelles pensées critiques*
– Naomi Klein, *No logo. La tyrannie des marques*
– Naomi Klein, *Tout peut changer. Capitalisme et changement climatique*
– Andrea Langlois et Frédéric Dubois (dir.), *Médias autonomes. Nourrir la résistance et la dissidence*
– Linda McQuaig, *Les milliardaires. Comment les ultra-riches nuisent à l'économie*
– Luc Rabouin, *Démocratiser la ville. Le budget participatif: de Porto Alegre à Montréal*
– Sherene H. Razack, *La chasse aux Musulmans. Évincer les Musulmans de l'espace politique*
– Jeremy Scahill, *Le nouvel art de la guerre. Dirty Wars*
– Astra Taylor, *Démocratie.com. Pouvoir, culture et résistance à l'ère des géants de la Silicon Valley*
– Lesley W. Wood, *Mater la meute. La militarisation de la gestion policière des manifestations*

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Robert LALIBERTÉ
a révisé le texte

L’epub et la mise en page sont
de claudebergeron.com

Lux Éditeur
C.P. 60191
Montréal (Québec) H2J 4E1
www.luxediteur.com

Clique ici pour plus de livres : https://t.me/formations8

Clique ici pour plus de livres : https://t.me/formations8

Il y a presque dix ans – avant WikiLeaks, Occupy Wall Street et le Printemps arabe –, l'anthropologue Gabriella Coleman se plongeait dans l'étude d'un phénomène mondial alors en pleine expansion: la communauté de hackers au masque désormais célèbre, Anonymous. Après quelques mois, elle était devenue si étroitement liée au groupe – tantôt confidente, tantôt interprète ou porte-parole – que ce statut ambigu, atypique, avait pris une place centrale dans son travail. C'est depuis cette zone liminaire que ce récit entreprend de cerner la nébuleuse, à la manière d'un journal d'enquête anthropologique.

Son immersion étonnante dans la sous-culture d'Anonymous, Gabriella Coleman l'enrichit de témoignages obtenus auprès de hackers célèbres en pleine action. S'y chuchote, dans l'ombre de la figure légendaire du *trickster*, la jubilation du *lulz* – le plaisir de jouer des sales tours, la délectation du *trolling*, l'exaltation de la piraterie. Une forme naissante et rageuse d'activisme s'y déclare aussi haut et fort, qui aura le succès que l'on connaît.

Sans rien céder aux charmes de l'anecdote, l'ouvrage pense plus largement l'action directe dans le cyberespace, en creusant notamment la question de l'éthique du hacking. Il examine dans le même temps les mécanismes de répression conçus par les autorités pour contrer cette nouvelle forme de contestation.

Cette étude sur Anonymous est indubitablement la plus complète et la plus rigoureuse existant à ce jour.

Docteure en anthropologie, Gabriella Coleman dirige aujourd'hui la chaire Wolfe en littératie scientifique et technologique de l'Université McGill. Elle est considérée comme la spécialiste d'Anonymous et intervient régulièrement dans les médias pour parler du phénomène et décrire les mécanismes coercitifs et les préjugés dont ils sont la cible.

FUTUR PROCHE

Clique ici pour plus de livres : https://t.me/formations8