UNIVERSITÉ DU QUÉBEC À MONTRÉAL

LE HACKTIVISTE: ENTRE BIDOUILLEUR ET CYBERTERRORISTE

MÉMOIRE

PRÉSENTÉ

COMME EXIGENCE PARTIELLE

DE LA MAÎTRISE EN COMMUNICATION

PAR

ANNE-SOPHIE LETELLIER

AVRIL 2015

REMERCIEMENTS

J'aimerais remercier plusieurs personnes formidables dont l'implication dans divers aspects de ma vie m'ont permis non seulement de compléter ce mémoire, mais surtout de passer deux premières merveilleuses années aux cycles supérieurs. Vous rendez, chacun à votre manière, les moments les plus difficiles en défis amusants et motivants. Vous avoir dans mon entourage est une chance inestimable.

J'aimerais également remercier Gabriella Coleman de m'avoir permis de participer à son séminaire portant sur les sous-cultures web à l'Université McGill. Ce mémoire n'aurait pas été le même sans son expertise et ses nombreux conseils sur la manière d'aborder la curieuse bête qu'est le collectif d'Anonymous. Un merci particulier à Normand Landry; merci de m'avoir permis de joindre à deux projets fascinants et d'avoir de ce fait grandement contribué à ma formation académique.

Finalement, un énorme merci à mon directeur, André Mondoux. Merci de ton accompagnement indispensable, de ta très grande disponibilité, de ta rapidité de correction, de la pertinence de tes commentaires et de ton grand support quand vient le temps d'aborder, de comprendre, d'apprécier et de vulgariser des auteurs dont les écrits semblent, à la première lecture, insurmontables. Je voudrais également te remercier d'avoir alimenté ma curiosité depuis ma première année de baccalauréat avec des lectures passionnantes et de m'avoir encouragé à faire des études supérieures. Je n'aurais probablement jamais considéré faire une maîtrise (encore moins un doctorat) si ça n'avait été de ta disponibilité, ton humour, ton enthousiasme et de ton enseignement.

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ABBRÉVIATIONS ET DES ACCRONYMES

ABC :	« American Broadcasting Company »
ACTA :	« Anti-Counterfeiting Trade Agreemet ». En français; Accord Commercial anti-contrefaçon.
CAE :	« Critical Art Ensemble »
CNN :	« Cables News Network »
CSEC :	« Communication Security Establishment Canada »
DdoS :	« Distributed Denial of Service »
EDT :	« Electronic Disturbance Theater »
FBI :	« Federal Bureau of Investigation »
IRC :	« Internet Relay Chat »
IP (Adresse) :	« Internet protocol »
LOIC :	« Low Orbit Ion Canon »
MPAA :	« Motion Picture Association of America »
MVDA :	« Mass Virtual Direct Action »
NBC :	« National Broadcasting Company »
NSA :	« National Security Agency »
NVDA :	« Non Violent Direct Action »
RIAA :	« Recording Industry Association of America »
TIC :	Technologie de l'information et de la communication

RÉSUMÉ

Ce mémoire s'intéresse à l'appropriation des technologies de l'information et de communication (TIC) par des groupes militants hacktivistes. Le hacktivisme (Jordan & Taylor, 2004; Coleman, 2012) est ici compris comme un usage tactique (de Certeau, 1990) des TIC dans un contexte de militance. En étudiant spécifiquement le cas l'*Operation : Payback* menée par le collectif Anonymous, cette recherche s'intéresse spécifiquement aux luttes sémantiques entourant le cadrage des mobilisations hacktivistes et des militants qui y prennent part. Effectivement, l'objectif principal est d'étudier de quelles manières les écarts entre le discours des médias de masse américains et celui des militants met en scène et véhicule des relations de pouvoir relatives non seulement à la gouvernance du cyberespace, mais à l'expansion de l'environnement stratégique néolibéral (de Certeau, 1990) dans son ensemble. À travers une analyse critique du discours, nous avancerons que les mobilisations d'Anonymous défient non seulement les codes techniques relatifs à l'usage des technologies numériques, mais aussi ceux relatifs aux normes culturelles de l'environnement stratégique néolibéral, notamment par l'importance de la notion de l'anonymat dans l'esthétisme et les pratiques organisationnelles du collectif. Les discours étudiés permettent finalement de mettre en scène des rapports de pouvoir où la notion de l'anonymat est centrale. En premier lieu, elle permet de mettre de l'avant, dans le discours des médias, l'image d'un collectif opaque, mystérieux et donc menaçant pour l'ordre en place. Ensuite, elle est nécessaire à l'édification de l'identité inclusive et idéologiquement perméable d'Anonymous et permet au collectif de se poser en tant que force transgressive en se dérobant aux pratiques de surveillance inhérentes au monde numérique.

Mots clés : hacktivisme, analyse de discours, Anonymous, désobéissance civile électronique, technologies numériques.

INTRODUCTION

Le hacktivisme comme mode de militance sur les technologies numériques a émergé dans les années 1990 dans les mobilisations altermondialistes du Electronic Disturbance Theater, du Critical Art Ensemble et des electro hippies (Dominguez, 2010; Jordan & Taylor, 2004; Sauter, 2014). Cependant, ce n'est qu'au cours de la première décennie du 21^{e} siècle que ce mode de militance devient *connu* aux yeux du grand public à travers notamment les pratiques du collectif Anonymous. À travers ses mobilisations contre, entre autres, l'Église de la Scientologie (2008), les multinationales PayPal, MasterCard et Visa (2010) puis dans ses implications numériques dans les révolutions du printemps arabe (2011), le collectif a attiré l'attention des médias et a fait couler beaucoup d'encre autour de ses mobilisations et de ses pratiques techniques controversées. Le présent mémoire s'intéresse donc au hacktivisme comme pratique de militance dans le contexte sociotechnique actuel. Le hacktivisme est ici entendu comme un répertoire d'action où l'appropriation tactique (de Certeau, 1990) des TIC permet une mobilisation autour d'enjeux politiques extérieurs aux systèmes informatiques. Ce répertoire d'actions conceptualise donc les TIC comme un espace et un outil propices à des activités de militance, où des tactiques sont déployées afin de restreindre les activités de l'adversaire sur les réseaux numériques (Söderberg, 2013) et autour de valeurs souvent inhérentes à l'émergence de l'Internet (anonymat, liberté de l'information et d'expression, propriété intellectuelle, méritocratie, décentralisation du pouvoir, etc.) et relatives à leur gouvernance. Par la nature souvent illégale de ses tactiques, le hacktivisme est associé à la désobéissance civile électronique (Costanza-Chock, 2003).

Cependant, les pratiques de *hacking* et de hacktivisme semblent récemment s'être conceptuellement rapprochées d'une menace cyberterroriste. Effectivement, plusieurs chercheurs remarquent une tendance chez les acteurs étatiques et corporatifs à élargir les frontières conceptuelles liées aux définitions du cyberterrorisme (Conway, 2007) de manière à identifier comme tel toute activité informatique illégale et politiquement motivée (Nelson et al., 1999). Le cadrage conceptuel et légal a donc le potentiel d'avoir des répercussions sur les sanctions attribuées aux militants tout en rapprochant dangereusement les frontières entre le *hacking,* le hacktivisme et le cyberterrorisme. Dans ce contexte, il devient particulièrement intéressant de se questionner sur les raisons qui expliquent un écart si important entre le cadrage des mobilisations hacktivistes par les militants — réclamant ces pratiques comme des modes de protestation légitime — et par les institutions politiques et les corporations – les criminalisant en les rapprochant conceptuellement du cyberterrorisme.

En comprenant les pratiques hacktivistes comme un usage tactique et détourné des technologies numériques (de Certeau, 1990) donnant lieu à un affrontement des stratégies opérées à travers le discours (Foucault, 1982), nous pouvons étudier les rapports de pouvoir inhérents au cadrage de ce type de pratiques militantes émergentes. Selon cette perspective, ce mémoire étudie le cas spécifique de l'*Operation : Payback,* mené par le collectif Anonymous en 2010 et en 2011, de manière à voir comment le cadrage de la mobilisation, du collectif et de ses militants permet l'édification d'un imaginaire populaire autour du sujet hacktiviste et de ses mobilisations. Ainsi, il a été question, à travers une analyse critique du discours, d'analyser deux discours entourant l'*Operation : Payback :* celui des militants et celui des médias de masse américains.

Une démarche exploratoire inductive a été utilisée dans ce mémoire avec l'objectif principal d'analyser la manière dont les discours véhiculent et mettent en scène des rapports de pouvoir relatifs à la fois à l'usage tactique des technologies numériques et

à la transposition des pratiques de militance dans le cyberespace. Autrement dit, il s'agit de problématiser les discours afin de soulever d'une part, les enjeux idéologiques inhérents à l'usage tactique des technologies numériques et, d'une autre part, les enjeux politiques, éthiques et organisationnels propres à ce type de militance politique. Il sera ainsi argumenté que l'usage tactique de la technique dans un contexte de militance engendre des rapports de pouvoir, relatifs non seulement à la gouvernance du cyberespace, mais à l'expansion du pouvoir stratégique d'un environnement néolibéral. Ces relations de pouvoir prennent forme, entre autres, alors que des militants transgressent explicitement plusieurs valeurs politiques, légales et culturelles de l'environnement néolibéral et que ce dernier évacue le caractère politique de ces mobilisations.

Enfin, le présent mémoire abordera le sujet en accordant une grande importance au contexte sociotechnique et politique dans lequel prennent place ces affrontements et dans lequel se positionne le discours des médias. Il sera ainsi question de positionner les objets techniques comme à la fois porteurs de valeurs et de discours, puis comme induisant une rationalité technique influençant les pratiques de gouvernance contemporaines. Nous verrons ensuite comment les pratiques hacktivistes viennent à la fois défier les valeurs portées par les objets techniques et poser le discours prétendument rationnel, neutre et non idéologique comme une production symbolique.

CHAPITRE 1 : PROBLÉMATIQUE DE RECHERCHE

Dès la fin de la Guerre Froide et de manière plus prononcée depuis l'émergence de l'Internet, l'information et ses réseaux sont propulsés « au cœur des doctrines sur la construction de l'hégémonie mondiale » (Mattelart, 2010, p. 11). Ainsi, si les technologies de l'information et de la communication (TIC) ont historiquement été au cœur des pratiques de gouvernance, alors il est nécessaire de leur reconnaître un rôle indubitablement redéfini, voire amplifié par l'usage des technologies numériques. Que ce soit par le développement de technologies de géolocalisation, par la transposition sur support numérique des documents des gouvernements et corporations ou par l'avènement du *Big Data*, les TIC induisent des rapports de pouvoir à plusieurs niveaux. D'une part, les données produites à travers l'usage des réseaux sociaux (i.e Facebook, Twitter, etc.) par les citoyens (diverses informations mises en ligne de manière volontaire concernant plusieurs aspects de la vie privée) deviennent propices à des pratiques de surveillance de la part de certains organismes gouvernementaux (tel qu'il a été le cas aux États-Unis avec la NSA[1], et au Canada avec le CSEC[2]) et d'entreprises utilisant les données générées par les utilisateurs afin de produire des publicités ciblées. D'autre part, le fait que les TIC contrôlent un nombre croissant d'aspects de la vie contemporaine rend plusieurs infrastructures (i.e banques, centrales électriques) et documents confidentiels vulnérables à des attaques informatiques (Clarke et Knake, 2011). Dans ce contexte, la communication n'est plus utilisée comme une simple préoccupation logistique, mais comme un enjeu

[1] Acronyme de National Security Agency. Les pratiques de surveillance menées par l'organisme ont été exposées par Edward Snowden via l'organisme Wikileaks

[2] Acronyme pour Communication Security Establishment Canada. L'homologue canadien du NSA, l'organisme est présentement poursuivi par la British-Colombia Civil Liberty Association pour atteinte à la vie privée des citoyens canadiens.

idéologique déterminant pour le maintien d'un pouvoir hégémonique (Mattelart, 2007). La gouvernance des technologies numériques (et des données qu'elles génèrent) devient donc un enjeu stratégique et induit des relations de pouvoir (Foucault, 1976) entre de multiples acteurs (citoyens, institutions étatiques et juridiques, agents corporatifs, etc.) issus de différents domaines (économique, politique, juridique, etc.). Dans cette optique, nous nous m'intéressons aux usages et au détournement des technologies numériques ainsi qu'aux rapports de pouvoir qu'ils sous-tendent.

Ce mémoire abordera précisément les rapports de pouvoir relatives aux mobilisations hacktivistes : plus spécifiquement celles de l'*Operation : Payback,* une opération menée par le collectif Anonymous entre les mois de septembre 2010 et janvier 2011. Le hacktivisme est ici entendu comme « la réappropriation des techniques de *hacking* informatique pour créer de nouvelles formes de militance politique » (Traduction libre : Jordan et Taylor, 2004, p. 2). De cette manière, il s'agira, en premier lieu, de comprendre les dispositifs techniques que sont les TIC comme des objets porteurs de rapports de pouvoir. En deuxième lieu, il sera question de problématiser l'usage détourné des TIC dans les mobilisations hacktivistes comme rapports de pouvoir. Ceux-ci seront problématisés en abordant les luttes sémantiques entourant le cadrage de *l'Operation : Payback* entre les médias de masse américains et les militants hacktivistes.

1.1 Discours, TIC et rapports de pouvoir

1.1.1 Foucault et le pouvoir

Afin de comprendre les TIC comme porteuses de discours, de valeurs et, conséquemment, de rapports de pouvoir, il importe de définir ce qui est entendu par *pouvoir* et de quelle manière il est lié au discours. Pour Foucault, le pouvoir n'est pas centralisé et n'est pas exercé à travers une seule structure, mais se déploie dans une multitude de relations. Ainsi, le pouvoir « vient d'en bas » et est exercé à travers des « rapports de force multiples qui se forment et jouent dans les appareils de production : les familles, les groupes restreints, les institutions, servent de supports à de larges effets de clivages qui parcourent l'ensemble du corps social. » (Foucault, 1976, p. 124). Les pratiques de gouvernance induites, à titre d'exemple, par l'État souverain ou par les différentes institutions politiques, juridiques et économiques formant les sociétés occidentales seraient édifiées à travers ce que Foucault qualifie des formes de « micropouvoir ». Il s'agirait donc d'un réseau complexe de rapports de pouvoir qui érigeraient les institutions qui gouvernent ensuite stratégiquement une société donnée à l'aide d'un ensemble de tactiques (Foucault, 1978). La tactique est comprise comme étant « la logique d'une pratique qui, à la différence de la stratégie, ne saurait être l'objet d'une légitimation discursive » (Resweber, 2004, p. 5). Conséquemment, la tactique relève de la pratique et du « faire sens » alors que la stratégie prend forme dans des dynamiques de confrontation visant à agir sur un adversaire de manière à déterminer sa conduite (Foucault, 1975), à le gouverner. Le pouvoir, selon Foucault, ne pouvant que se poser qu'en matière de rapports, désigne en ce sens « une relation entre partenaires [...], un ensemble d'actions qui s'induisent et se répondent les unes aux autres » (Foucault, 1978, p. 1052). En tenant donc pour acquis que le pouvoir n'est pas une forme de domination, contraignant physiquement des sujets à agir d'une certaine manière, mais un rapport exercé envers des sujets dits

libres, il est nécessaire de le conceptualiser en tenant compte des pratiques de résistance qui le composent :

> Il n'y a pas de relations de pouvoir sans résistance, sans échappatoire ou fuite, sans retournement éventuel, toute relation de pouvoir implique donc, au moins de façon virtuelle, une stratégie de lutte, sans que pour autant elles en viennent à se superposer, à perdre leur spécificité et finalement à se confondre. Elles constituent l'une pour l'autre une sorte de limite permanente, de point de renversement possible (Foucault, 1978, p. 1061).

La gouvernance et l'usage (acteurs humains) des TIC (acteurs non-humains) peuvent ainsi être perçus comme une forme de « micropouvoir » se rattachant à un réseau beaucoup plus vaste de rapports de pouvoir.

Le discours, quant à lui, est un élément dans le dispositif stratégique des rapports de pouvoir, le pouvoir étant quelque chose « qui opère à travers le discours » (Foucault, 1978, p. 465). De cette manière, Foucault soutient que le discours relève d'un jeu, d'un assemblage d'énoncés structurés de manière à le rendre prévisible. Le fait de choisir une série d'énoncés parmi la totalité des énoncés possibles relève donc directement du pouvoir. Selon cette perspective, le pouvoir opérant à travers le discours sert à construire la réalité d'acteurs individuels et collectifs en devenant une manière de gouverner, c'est-à-dire de gérer les possibilités et de rendre prévisibles certains types de conduite parmi l'ensemble de conduites possibles :

> « [le pouvoir] est un ensemble d'actions sur des actions possibles : il opère sur le champ de possibilité où vient s'inscrire le comportement de sujets agissant ; [...] il est bien toujours une manière d'agir sur un ou sur des sujets agissants, et ce tant qu'ils agissent ou qu'ils sont susceptibles d'agir. Une action sur des actions. » (Foucault, 1982, p. 1056)

Ici, la notion de « code technique », telle que conceptualisée par Andrew Feenberg (Feenberg, 2004), sera mobilisée pour décrire les valeurs, les normes et les discours matérialisés dans les TIC. Effectivement, ces codes appartenant à un environnement stratégique tendent par leur structure technique à prescrire aux utilisateurs certains

types d'actions, un certain usage parmi tous les usages possibles. Inversement, les utilisateurs peuvent détourner ou s'approprier ces mêmes codes à d'autres fins, rendant de ce fait les TIC tributaires de rapports de pouvoir.

1.1.2 La stratégie et la tactique

Les notions de stratégies et de tactiques abordées dans plusieurs travaux de Michel Foucault sont également mobilisées par Michel de Certeau. Ce dernier a commenté, cité et critiqué à plusieurs reprises les œuvres de Foucault (Resweber, 2004). Dans « *L'invention du quotidien* » (de Certeau, 1990), il reprend effectivement les notions de tactique et de stratégie en soulignant les « multiples interactions existant entre les pratiques et les discours et dont rendent compte les pratiques discursives » (Resweber, 2004, p. 2) en interposant cependant « les pratiques [aux] formations discursives qui les commandent » (Resweber, 2004, p. 2).

Pour de Certeau, les rapports de pouvoir induits par l'architecture et la gouvernance des TIC se rattacheraient à l'expansion du pouvoir *stratégique*. Ici, l'usage stratégique des TIC relève de l'implantation et de la normalisation de codes techniques à l'intérieur d'un environnement donné :

> J'appelle « stratégie » le calcul des rapports de force qui devient possible à partir du moment où un sujet de vouloir et de pouvoir est isolable d'un « environnement ». Elle postule un lieu susceptible d'être circonscrit comme un propre et donc de servir de base à une gestion de ses relations avec une extériorité distincte. La rationalité politique, économique ou scientifique s'est construite sur ce modèle stratégique (de Certeau, 1990, p. 59).

Un environnement ainsi que les codes qui le composent sont donc définis par la production de règles, de lois, de valeurs propres à un type de discours, à une stratégie. Alors que Foucault décrit la tactique comme une « logique de la pratique » engendrant des confrontations stratégiques, de Certeau la conceptualise comme relevant de l'appropriation, de la ruse ou du « braconnage » à l'intérieur d'un

environnement stratégique. Pour lui, la tactique appartient plutôt aux pratiques marginales, individuelles et isolées.

Dans ce mémoire, il sera question de mettre en relation ces deux conceptualisations de la stratégie et de la tactique. L'une étant davantage liée au discours alors que l'autre étant liée à l'usage, il sera question d'aborder initialement le hacktivisme comme un usage tactique des TIC dans un environnement stratégique donné. Cependant, bien que l'usage des technologies numériques puisse être qualifié de tactique, il n'en reste pas moins que, dans le cas des mobilisations hacktivistes, cet usage semble s'inscrire dans des relations de pouvoir entrainant des confrontations stratégiques. Autrement dit, les pratiques hacktivistes s'apparentent davantage à ce que de Certeau qualifie d'usage tactique, alors que les pratiques discursives les entourant s'inscrivent plutôt dans une dynamique d'affrontement des stratégies (Foucault, 1978).

1.1.3 Environnement stratégique et adversité politique

Dans cet ordre d'idée, il s'avère pertinent d'aborder la notion de construction d'un environnement stratégique dans lequel les codes techniques sont défiés par les tactiques hacktivistes. À cet égard, la notion de construction de l'identité politique abordée par Chantal Mouffe dans l'ouvrage « *On the Political* » (Mouffe, 2005) s'avère particulièrement intéressante et peut ainsi être rattachée à la construction d'un environnement stratégique. L'auteure soutient effectivement que l'identité se construit à travers des dynamiques relationnelles à l'Autre (Mouffe, 2005), à une extériorité distincte. Le fondement d'une identité, c'est-à-dire la construction du « nous », est nécessairement lié aux processus discursifs qui, en mettant de l'avant un jeu de structures, de normes et de codes, fondent des règles plus ou moins explicites d'inclusion. Ces normes ne peuvent cependant qu'être construites en fonction de ce qui leur est extérieur. Ainsi, la construction d'une identité s'opère en identifiant ce

qui est intérieur d'un environnement. En contrepartie, elle doit également définir ce qui constitue son extérieur, c'est-à-dire le « eux ». Dans le contexte actuel, c'est dire que la légalité ne peut être définie que relativement à l'illégalité; la moralité, avec l'immoralité; le bien avec le mal, etc.

En ce sens, Mouffe conceptualise deux types d'adversité politique. La première en est une agoniste dont la relation « nous/eux » est basée sur le fait que les opposants reconnaissent la légitimité de leurs adversaires (Mouffe, 2005, p. 20). La seconde est une adversité antagoniste qui, contrairement à l'adversité agoniste, se définit comme un « we/they relation in which two sides are ennemies who do not share any common grounds. [...] We would say that the task of democracy is to transform antagonism into agonism » (Mouffe, 2005, p. 20). Si l'adversité antagoniste marque les limites claires de tout consensus rationnel, le fait de ne pas reconnaître la possibilité d'une adversité antagoniste relève spécifiquement des valeurs à la fois portées par l'idéologie néolibérale actuelle et est également constitutive de celle-ci : « as far as liberal though adhers to individualism and rationalism, its blindness to the political in its antagonistic dimension is therefore not a mere empirical omission, but a constitutive one » (Mouffe, 2005, p. 12). De par son caractère global, l'idéologie néolibérale construit discursivement son identité avant tout par l'impossibilité de se retrouver en son extérieur. Dans cet ordre d'idées, l'Autre est discursivement construit en termes d'immoralité et d'illégalité plutôt qu'en termes de discours politique : « [T]he political is played out in the moral register. [...] [T]he we/they, instead of being defined by political categories, is now established in moral termes. In place of a struggle between 'right' and 'left', we are face with a struggle between 'right' and 'wrong' » (Mouffe, 2005, p. 5). Cette catégorisation a ainsi un impact important sur la légitimation des discours politiques antagonistes, ceux-ci n'étant pas, dans le contexte actuel, reconnus comme *légitimes,* mais plutôt illégaux et immoraux.

1.1.4 Rationalité technique et gouvernance des TIC

En prônant l'illégitimité des discours politiques antagonistes, la stratégie véhiculée à travers les discours néolibéraux vise avant tout à l'occlusion du politique, c'est-à-dire qu'elle vise à empêcher une remise en question des « codes techniques ». Ceux-ci deviennent non plus politiques, mais ontologiques. Ainsi, les discours façonnant l'environnement stratégique néolibéral seraient véhiculés à travers les objets techniques. Ceci rejoint ce que Jodi Dean qualifie de capitalisme communicationnel[3]. Effectivement, ce dernier se présente comme la matérialisation des discours néolibéraux dans les réseaux de la communication (Dean, 2003). À ce titre, si les technologies numériques se présentent comme étant potentiellement porteuses d'idéaux démocratiques (outils permettant la libre expression, la diffusion d'informations, etc.), elles restent néanmoins techniquement structurées et leur usage est gouverné dans le but d'assurer avant tout la liberté des marchés.

Ainsi, si ces valeurs sont véhiculées dans les structures des réseaux numériques, il est également pertinent de constater comment, de manière complémentaire, les processus techniques mobilisés dans ces technologies sont utilisés pour légitimer ces discours. Effectivement, l'universalisation des valeurs néolibérales vient en ce sens s'ancrer dans ce que Feenberg et Marcuse appellent une rationalité technique (Feenberg, 2004; Marcuse, 1968). Celle-ci défend un discours idéologique prétendument *rationnel* et *non idéologique* (Mondoux, 2011; Freitag, 2008). L'environnement stratégique serait légitimé à travers les processus techniques des technologies numériques. Cela renvoie à ce qui est soutenu par Alexander Galloway dans l'ouvrage *Protocol :*

> In what Michel Foucault called the sovereign societies of the classical era, characterized by centralized power and sovereign fiat, control existed as an

[3] Traduction libre à partir du terme anglais « Communicative capitalism »

> extension of the world and deed of the master, assisted by violence and other coercive factors. Later the disciplinary societies of the modern era took hold, replacing violence with more bureaucratic forms of command and control (Galloway, 2004, p. 4).

De cette manière, l'environnement stratégique propre aux discours néolibéraux serait soutenu par la structure TIC tout en étant légitimé par la rationalité et l'objectivité de leurs procédures techniques. Toujours selon Jodi Dean, les rapports de pouvoir induits à la fois par les structures légales, techniques et économiques entourant la gouvernance des TIC rendraient les pratiques de résistance particulièrement ardues; les usagers n'ayant d'autres choix que d'utiliser les codes techniques et les outils en place pour militer :

> Changing the system, organizing against and challenging communicative capitalism, seems to require strengthening the system : how else to get out the message than to raise the money, buy the television time, register the domain names, build the websites, and craft the accessible, user-friendly, spectacular message ? (Dean, 2003, p. 102)

Dans cette mesure, il devient particulièrement pertinent de se pencher sur le détournement et la transgression des codes techniques par des groupes militants. Les pratiques de militances basées sur les réseaux informatiques seront donc abordées en étudiant comment l'usage détourné des TIC se pose en opposition au pouvoir stratégique des discours néolibéraux.

1.1.5 Le hacktivisme comme pratique de militance

Dans ce mémoire traitant spécifiquement du hacktivisme, le terme sera défini comme un répertoire d'actions où l'appropriation et le détournement technique des TIC par des techniques de *hacking* permettent une mobilisation en ligne autour d'un discours politique et d'enjeux communs souvent associés aux valeurs inhérentes à l'émergence du web (anonymat, liberté de l'information et d'expression, propriété intellectuelle, méritocratie, décentralisation du pouvoir, etc.). Il met de l'avant à la fois un discours politique et des actions techniques qui le remettent en question ou, du moins,

prouvent son extériorité. Le hacktivisme est rattaché à des pratiques de militance politique en proposant un répertoire d'actions basé sur l'Internet. Les répertoires d'actions *basés sur l'Internet* utilisent les TIC comme objet et outil de mobilisation. D'une part, leur gouvernance et leur usage font émerger de nouvelles problématiques et, d'autre part, elles deviennent un lieu où des outils techniques sont détournés afin de restreindre les activités d'adversaires sur les réseaux numériques.

Les premières mobilisations hacktivistes datent des années 1990 (Critical Art Ensemble, 1996; Dominguez, 2010). Celles-ci étaient cadrées par les activistes comme des actes de *désobéissance civile électronique* (Costanza-Chock, 2003) et perçues comme un répertoire d'actions complémentaire aux mobilisations hors-ligne (Sauter, 2013). La principale tactique de désobéissance civile électronique mise de l'avant par les premiers groupes hacktivistes a été action par déni de service[4], qui peut être vulgarisée comme étant un *sit-in* électronique. Selon Sasha Costanza-Chock, une action par déni de service est une pratique résultant en un « blockage of public access to the target site [...]. When targets are companies that rely on online sales, such actions can have significant economic as well as symbolic impact » (Costanza-Chock, 2003, p. 6). Mis simplement, il s'agit d'envoyer des séries de demandes d'accès à un site web jusqu'à ce que ce dernier soit ralenti ou jusqu'à ce qu'il ne soit plus en état de fonctionner. Il est également à noter que le choix du terme « action » pour référer à la tactique n'est pas anodin. Comme Molly Sauter dans son livre « The Coming Swarm », nous choisissons de nommer la tactique comme une « action » plutôt que comme une « attaque ». Effectivement, tel que le note Sauter, « by referring to all DDoS actions, regardless of motivations as ''attacks'', the public, law enforcement, and even practitioners are primed to think of DDoS actions in terms of violence, malice, and damage » (Sauter, 2014, Empl. 240).

[4] Voir glossaire

La tactique a été utilisée par des mouvements altermondialistes tels que le *Electronic Disturbance Theater*[5] (EDT) dans le contexte des soulèvements zapatistes dans le Chiapas au Mexique (Dominguez, 2010) et les *electrohippies*[6] lors des émeutes du *World Trade Organisation* à Seattle en 1999 (Taylor et Jordan, 2003). Le logiciel développé et utilisé par le EDT pour mener ces actions, nommé le *FloodNet*[7], s'inscrivait par son interface dans une continuité logique des protestations hors-ligne. Effectivement, l'outil était configuré pour affecter uniquement une série de sites web « néolibéraux » préalablement sélectionnés par le EDT. De plus, l'envoi d'informations vers le serveur cible devait être déclenché manuellement par un individu à un ordinateur – chaque flot d'informations devait donc être issu d'une seule personne dans l'optique d'assurer la légitimité de la mobilisation.

1.1.6 Anonymous

Dans ce mémoire, le cas du collectif hacktiviste Anonymous sera étudié. Celui-ci s'est fait connaître dans ses mobilisations contre, entre autres, l'Église de la Scientologie, Visa, MasterCard et PayPal. Ces mobilisations ont fait couler beaucoup d'encre et ont certainement permis aux hacktivistes d'occuper une place importante dans le paysage médiatique contemporain et rendant de ce fait les problématiques liant cyberespace et militance plus visible au public (Coleman, 2013).

Le collectif Anonymous, représenté comme des réseaux décentralisés de « chiens de garde » de l'Internet, comme les « *mauvais garçons* » ou les « *motherfuckers* » de l'activisme politique (Coleman, 2013), a émergé depuis la plateforme/b/[8]de

[5] Voir glossaire
[6] Voir glossaire
[7] Voir glossaire
[8] Voir glossaire

4chan.org[9] (Coleman, 2012; Phillips, 2013a). 4chan.org est un site web composé de pages (« boards ») où les utilisateurs publient sous le pseudonyme « *Anonymous* » des images ou des billets. Bien que le site soit composé de plusieurs « pages » aux thématiques variées (i.e dessins animés japonais, voyage, mouvement LGBT, activités paranormales, etc.), la plateforme qui nous intéresse est ici la plateforme/b/, la page aléatoire ou, en anglais, « random ». Elle est un lieu où circulent des discours dérangeants, et des images violentes et obscènes; le contenu présenté sur la plateforme étant contrôlé de manière minimale par les administrateurs du site.

À compter de 2003, le pseudonyme *Anonymous* devient populaire et est rapidement approprié par un groupe autodésigné et décentralisé qui l'utilise pour *des activités de trolling*[10] (Knuttila, 2013 ; Philipps, 2013b). Bien que le *trolling* ne se résume pas aux activités menées sur 4chan.org[11], nous nous concentrerons néanmoins sur la littérature portant sur les formes de *trolling* issues de cette plateforme puisque les écrits sur le collectif lient unanimement l'émergence du collectif à cette plateforme. Le *trolling* informatique consiste à viser de manière plus ou moins aléatoire des individus ou des groupes d'individus actifs sur l'Internet dans le but de les faire enrager autant que possible (Philipps, 2013b). À travers des pratiques transgressives et provocantes, ainsi qu'avec un indéniable sens du spectacle, les activités des trolls[12] sont opérées dans l'optique d'en retirer du *lulz,* « a cheap laught to someone elses expend » (Coleman, 2012). En termes plus familiers, les trolls peuvent être décrits comme des antihéros « who fuck things up » et leurs actions, comme du « motherfuckery » ultra coordonné (Coleman, 2012, p. 99). Les actions transgressives, les paroles diffamatoires utilisées par les trolls au nom du *lulz*, sont

[9] Voir glossaire
[10] Voir glossaire
[11] Elles prennent place sur une multitude de plateformes (jeux vidéo en ligne, forums divers, Facebook, Twitter, You Tube, etc.). De plus, les actes de *trolling* peuvent prendre plusieurs différentes formes, dépendant des groupes menant les opérations et les plateformes, les individus ou les groupes ciblés par les actions.
[12] Voir glossaire

associées à une violence verbale, pouvant rencontrer la définition légale du harcèlement (Coleman, 2010). Entre 2003 et 2008, ces actions prennent tranquillement un caractère politique en ciblant des individus tels que l'animateur de radio suprématiste blanc Hal Turner, des pédophiles, etc. (Jenkins, 2007)

Les pratiques d'Anonymous sont ainsi liées au trolling par leur esthétique et leur forme. Cependant, le mode d'organisation « secret » et décentralisé (via les Internet Relay Chat[13]), les valeurs liées à l'éthique des *hacker* et, bien entendu, l'usage tactique des TIC relèvent indubitablement du *hacking* informatique. Il ne va pas sans dire que leurs pratiques techniques, telles que les actions par déni de service, sont également directement liées aux pratiques hacktivistes de leurs prédécesseurs (Hacktivismo, Electronic Disturbance Theater, Electrohippies, etc.).

Anonymous se pose ainsi comme un groupe transgressif à plusieurs niveaux : techniquement par les activités de *hacking* souvent illégales ; culturellement par le langage vulgaire utilisé par les trolls, associé à l'immoralité ; et politiquement par leur manière de défier les codes techniques propres à l'environnement stratégique duquel ils émergent. Les tactiques les plus souvent utilisées dans les mobilisations d'Anonymous s'avèrent être de surprenantes combinaisons (légales et illégales) de « telephone pranking », d'envoi de pizzas non payées à l'adresse d'une cible, d'action par déni de service et de mise en ligne d'informations personnelles (*doxing*) et préférablement humiliantes (Coleman, 2012).

[13] Voir glossaire

1.2 Problématique de recherche

Si les *hacker* ont déjà été associés à une figure de virtuosité technique et de curiosité ayant façonné la *révolution informatique* (Levy, 1984), ceux-ci semblent actuellement associés dans l'imaginaire populaire à la figure du pirate, à celle du criminel. Le fait que ces derniers puissent maitriser les machines contrôlant de nombreux aspects de la vie contemporaine et dont le fonctionnement, aux yeux de la population en général, relève de la plus grande abstraction (Hafner & Markoff, 1995) rend leurs actions ainsi que l'impact de celles-ci complètement imprévisibles, donc menaçantes. De manière plus importante, cette conception semble servir à criminaliser tout usage détourné ou non permis des ordinateurs et des TIC, peu importe leur motivation ou leurs fins (fraude électronique, vol de données, interruption temporaire des réseaux, ou intrusion sans vol ni destruction de données) (Conway, 2008). À titre d'exemple, le terme *cracker* a longtemps désigné les *hacker* capables d'entrer illicitement dans un système informatique dans le but de démontrer leurs connaissances, pour signifier les faiblesses sécuritaires ou pour satisfaire une simple curiosité personnelle. Aujourd'hui, le terme sert également à décrire la fraude électronique et les crimes informatiques dans leur sens le plus large (Conway, 2008). Ce néologisme est donc utilisé pour signifier le *craquage* d'un code informatique autant que pour regrouper les concepts de crime et de *hacking* informatique, confondant ainsi sous le même nom, les pratiques frauduleuses et tout acte d'entrer illicitement dans un réseau (sans pour autant altérer ou voler des données).

Un rapprochement semblable tend à être fait entre les pratiques de hacktivisme et de cyberterrorisme (Conway, 2008). Compte tenu de l'importance des réseaux de l'information dans les sociétés contemporaines et dans la foulée des événements du 11 septembre 2001, la perspective que des *hackers* puissent s'adonner à des activités s'apparentant au cyberterrorisme devient une menace motivant l'élaboration de stratégies de défenses par des acteurs gouvernementaux et corporatifs. Plusieurs

auteurs notent cependant une grave lacune quant à la conceptualisation du terrorisme et, par conséquent, du cyberterrorisme (Conway, 2008). Alors que plus de 80 % des chercheurs semblent être d'accord sur ce qui constitue le terrorisme – la violence envers des civils, la recherche de la peur pour atteindre un objectif politique et la motivation politique – (Conway, 2009), très peu conviennent d'un terrain d'entente en ce qui a trait à la conceptualisation du cyberterrorisme.

Ainsi, la manière dont les médias, les institutions gouvernementales et les acteurs corporatifs mobilisent cette notion tend à élargir dangereusement le spectre des actions pouvant être potentiellement qualifiées de cyberterroristes, jusqu'à presque totalement évacuer la menace relative à l'intégrité physique des civils – associé aux attaques terroristes dites traditionnelles — au profit d'une attaque à la propriété physique ou intellectuelle. Dans certains cas, ces attaques à la propriété peuvent être réduites aux crimes informatiques et à des pratiques de fraude électronique (Conway, 2009; Nelson et coll., 1999; Fox News, 2010).

Selon cette perspective, il est possible de noter les frontières floues entourant la conceptualisation des différentes pratiques de *hacking.* Par exemple, l'élargissement des frontières du cyberterrorisme permet de rattacher à ce concept toute activité informatique illégale et politiquement motivée (Conway, 2008; Nelson et al, 1999). De plus, le fait qu'une section du Patriot Act[14] soit dédiée aux crimes informatiques — stipulant que toute intrusion dans les systèmes informatiques peut être considérée comme du terrorisme et poursuivie en justice comme telle (Young et al, 2007) – démontre que le cadrage conceptuel et juridique des pratiques de *hacking* a le potentiel d'avoir de grandes répercussions sur les sanctions attribuées aux *hackers,*

[14] Acronyme d'un acte de congrès signé le 26 octobre 2001 sous la présidence de George W. Bush afin de prévenir d'éventuelles attaques terroristes : **U**niting and **S**trengthening **A**merica by **P**roviding **A**ppropriate **T**ools **R**equired to **I**ntercept and **O**bstruct **T**errorism Act of 2001.

tout en rapprochant dangereusement les frontières entre le *hacking,* le hacktivisme et le cyberterrorisme.

1.2.1 L'image des hackers

L'association faite dans l'imaginaire populaire entre le pirate et le *hacker* s'avère très révélatrice : le premier est associé à des groupes n'appartenant à aucune nation, volant des richesses dans les eaux internationales en proclamant que celles-ci relèvent du bien commun; le second est rattaché à des individus utilisant les réseaux informatiques afin d'entrer illicitement sur des systèmes et pour potentiellement voler du matériel protégé (Liang, 2010). Ainsi, peu importe ses intentions (fraude, curiosité, sécurité, activisme politique), le *hacker* transgresse les limites et les codes techniques d'un environnement stratégique.

Effectivement, les *hackers* et leurs pratiques techniques, tout comme les référents culturels et moraux qui en sont issus, ont historiquement joué avec les frontières de la légalité. Par leur curiosité et leur grande capacité d'innovation, « les actions des *hackers* et leurs artéfacts sont généralement dans des zones grises de la loi ou remettent en cause ce qui est illégal. Dans tous les cas, ils rendent visibles ou contentieux plusieurs dilemmes » (Traduction libre : Coleman, 2012, p. 19). Leur caractère transgressif fait donc émerger ces contradictions inhérentes à l'Internet : l'Internet est-il un lieu de libre expression ou un outil de censure; est-il un espace public, un lieu de renouveau démocratique ou un lieu de surveillance; est-il un espace libre ou un espace marchand?

Ainsi, compte tenu de l'importance des réseaux de télécommunication, et par la « menace » croissante du cyberterrorisme, il n'est pas surprenant que les *hackers* soient plus facilement perçus comme des menaces au maintien de l'ordre en place. Effectivement, selon la *National Association of Criminal Defense Lawyers*, les

sentences attribuées aux crimes informatiques sont souvent disproportionnelles au crime opéré : « punishment for computer crimes often exceeds the seriousness of the offense by relying on inflated damage figures. Legislators hope that severe punishment will deliver a message to hackers around the world and serve as a deterrent for future crimes » (Young et coll., 2007, p. 281). Selon cette perspective, les mobilisations du collectif Anonymous seront abordées en portant une attention particulière à la manière dont les médias cadrent[15] les pratiques hacktivistes et à la manière dont ces mobilisations et l'image d'Anonymous sont discursivement associées à d'autres pratiques de *hacking*.

1.2.2 Positionnement de la recherche dans la littérature

La présente recherche se positionne à l'intersection de trois corpus de littérature. Le premier corpus traite spécifiquement du cadrage des pratiques de *hacking* dans les médias et par les institutions étatiques. Ces ouvrages se concentrent sur une période historique allant de 1950 à 2005 (Levy, 1984; Sterling, 1992; Hafner et Markoff, 1995; Denning, 2001; Conway, 2008, 2009; Liang, 2010; Mondoux, 2011). Le deuxième corpus est formé majoritairement des travaux ethnographiques de Gabriella Coleman portant spécifiquement sur Anonymous et les sous-cultures (i.e trolling, phreaking, etc.) du web desquelles le collectif a émergé (Coleman, 2010, 2011, 2012a, 2012 b, 2013; Philipps, 2013a, 2013 b). Finalement, le troisième corpus de littérature traite des mobilisations en ligne et de la désobéissance civile électronique, dans une perspective de mouvements sociaux. C'est-à-dire que ces ouvrages posent des problématiques relatives à la légitimation des répertoires d'action hacktivistes. Ils permettent donc d'établir un cadre pour analyser la légitimité de ces actions, mais

[15] Les termes « cadrer » et « cadrage » font référence dans ce mémoire au concept anglais « framing » qui, appliqué au domaine des sciences sociales, est lié à la construction sociale d'un concept via la perception, la compréhension et la communication de la réalité par des individus ou des collectivités (Goffman, 1974)

abordent uniquement la question de la désobéissance civile électronique en regard des mobilisations des années 1990 (Critical Art Ensemble, 1996; Costanza-Chock, 2003; Taylor et Jordan, 2004; Jordan, 2008; Dominguez, 2010; Söderberg, 2013).

1.2.3 Question et sous-questions de recherche

La problématique se fonde sur quatre constatations relevées précédemment :

1) La gouvernance des réseaux numériques relève d'un enjeu stratégique de pouvoir;
2) Les pratiques de *hacking*, tout comme les mobilisations hacktivistes, sont éminemment transgressives et souvent illégales;
3) Il existe une confusion générale autour de la conceptualisation et du cadrage des différentes pratiques de *hacking* informatique et de leurs impacts potentiels;
4) Les pratiques de *hacking* en général sont punies et jugées par les institutions juridiques de manière disproportionnelle aux crimes commis.

Selon cette perspective, la problématique de recherche se fonde sur l'écart existant entre le désir des hacktivistes à présenter leurs pratiques comme des modes de militance légitimes et la tendance qu'ont plusieurs acteurs gouvernementaux et corporatifs, à les criminaliser et à les rapprocher d'actes de cyberterrorisme (Costanza-Chock, 2003). Il est également particulièrement intéressant de se questionner sur l'écart potentiel entre le cadrage de ces actions par les pratiques discursives des militants et celles des médias de masse : les deux types de discours véhiculant des rapports de pouvoir visant la construction de la réalité d'acteurs individuels et collectifs (Foucault, 1978) relative, entre autres, à la gouvernance du cyberespace et à l'usage des TIC dans un contexte de militance politique.

En ce sens, la question de recherche proposée se formule comme suit : en étudiant les discours des médias de masse américains et ceux des militants, comment le cadrage de l'*Operation : Payback,* menée par le collectif hacktiviste Anonymous, témoigne-t-il de rapports de pouvoir relatifs non seulement à la gouvernance du cyberespace, mais à l'expansion du pouvoir stratégique du discours néolibéral?

Les discours mis de l'avant par les médias et par les militants seront analysés à travers des documents médiatiques. Ceux-ci tenteront de répondre aux sous-questions suivantes :

1) Comment est présenté le collectif Anonymous à travers les discours des médias de masse américains et celles des militants?

2) Comment est décrite l'*Operation : Payback* dans les discours des médias de masse américains et celles des militants?

3) Comment les revendications politiques et pratiques techniques du collectif Anonymous remettent-elles en question les codes techniques de l'environnement stratégique néolibéral?

4) Quels sont les enjeux sociopolitiques, éthiques, sécuritaires, économiques et légaux utilisés dans les discours de ces médias et dans celui des hacktivistes afin de supporter leurs cadrages respectifs des mobilisations?

1.2.4 Pertinence communicationnelle

Le projet de mémoire compte ainsi deux enjeux communicationnels majeurs. Il s'agit premièrement de comprendre l'usage détourné des TIC comme relevant d'une nouvelle conceptualisation du cyberespace par des militants. Il représenterait à la fois

un espace de communication tactique, un objet de mobilisation ainsi qu'un outil pour contraindre politiquement un adversaire en permettant l'action politique directe.

De manière plus importante, le second enjeu communicationnel relève de la lutte sémantique relative au cadrage des pratiques militantes dans le cyberespace et des stratégies communicationnelles mobilisées par certains acteurs afin de cadrer ces pratiques comme légitimes ou illégitimes; comme légales ou criminelles. Bref, ces deux enjeux permettent d'aborder ce que Sidney Tarrow relève comme des enjeux sous-étudiés dans l'étude des rapports de pouvoir dans les mobilisations contentieuses : celui du rôle et de l'usage des TIC dans l'innovation des répertoires d'actions militantes et celui des stratégies de répression par l'environnement stratégique néolibéral (Tarrow, 2010).

CHAPITRE 2 : CADRE THÉORIQUE

Puisque ce mémoire a pour objectif d'analyser les discours véhiculés par les médias et ceux véhiculés par les groupes hacktiviste, le présent cadre théorique sera composé de deux parties principales. La première partie définira l'environnement stratégique dans lequel prennent place les mobilisations hacktivistes. La seconde partie établira une grille d'analyse relative à la désobéissance civile électronique et à la transgression dans un contexte de militantisme. Deux axes seront exploités afin de rendre compte des rapports de pouvoir. Le premier axe relève de la nécessité d'un groupe à se construire une identité liée l'identification de l'« Autre » (Mouffe, 2005). Le second axe, la légitimité, relève directement du discours justifiant le cadrage, et sert à rendre une identité, une stratégie, et les codes qui la composent plus puissants. Il sera subséquemment argumenté que l'architecture des objets techniques est définie par des codes propres à un environnement stratégique et que les codes sont à leurs tours légitimés par les processus techniques. Finalement, il sera argumenté que l'usage tactique de la technique par les hacktivistes engendre des rapports de pouvoir relatifs non seulement à la gouvernance du cyberespace, mais à l'expansion de l'environnement stratégique néolibéral.

2.1 Usage stratégique de la technique et gouvernance

2.1.1 Environnement stratégique et le système-monde

Dans un premier temps, il sera question de constater comment les codes techniques servent à l'identification et à la délimitation d'un environnement stratégique. Plus précisément, l'environnement stratégique dans lequel prennent place les rapports de pouvoir entre les discours des hacktivistes et ceux des médias de masse américains sera conceptualisé en tant que système-monde (Mondoux, 2007). Le système-monde

relèverait d'une configuration idéologique où la rationalité technique servirait à induire et à légitimer une stratégie, un mode de gouvernance qui « se déploie dans et par le terroir sociohistorique, plus précisément par le biais de l'idéologie néolibérale » (Mondoux, 2012). Afin d'aborder les discours des hacktivistes et celui des médias comme des rapports de micropouvoir façonnant des rapports à l'échelle globale, l'idée selon laquelle le concept du système-monde relèverait d'une configuration idéologique édifiée à partir de nombreux rapports de pouvoir rejoint la pensée de Foucault :

> [C]es rapports de force trouvent [des appuis] les uns dans les autres, de manière à former une chaîne ou système, ou, au contraire, les décalages, les contradictions qui les isolent les uns des autres; les stratégies enfin dans lesquelles ils prennent effet, et dont le dessin général ou la cristallisation institutionnelle, prennent corps dans les appareils étatiques, dans la formulation de la loi ou dans les hégémonies sociales (Foucault, 1976, p. 122).

De cette manière, l'objet d'étude sera compris non pas comme des relations découlant directement des rapports de force induits par les modes de gouvernance du système-monde, mais plutôt comme un événement dans lequel les discours sont un véhicule (parmi d'autres) de rapports de pouvoir, qui s'inscrivent et participent à l'édification de structures dans l'environnement stratégique néolibéral. Nous verrons subséquemment comment les actions hacktivistes visent à résister et/ou à s'inscrire dans cette dynamique sociotechnique et politique contemporaine.

2.1.1.1 Les legs de la pensée cybernétique

Il est important de noter que l'objectif des prochains paragraphes n'est pas de comprendre les dynamiques politiques contemporaines selon une logique systémique. Il s'agit plutôt de voir comment les stratégies et les modes de gouvernance contemporains sont supportés par des discours qui se conçoivent comme ontologiques, c'est-à-dire ayant la prétention d'incarner un monde en soi. À ce titre, il

s'avère nécessaire de remonter à la pensée cybernétique afin de concevoir adéquatement de quelles manières l'information et son contrôle se sont avérés devenir des enjeux politiques dans l'environnement stratégique néolibéral contemporain.

La pensée cybernétique conçoit que le système informatique fonctionne de manière similaire à une société, où l'information qui y circule doit être contrôlée et gérée afin de pouvoir opérer le système à son plein rendement. Effectivement, la principale thèse de Norbert Wiener, le père de la cybernétique, « est que le fonctionnement physique de l'individu vivant et les opérations de certaines machines de communication (...) sont exactement parallèles dans leurs efforts identiques pour contrôler l'entropie par l'intermédiaire de la rétroaction » (Wiener, 1965, p. 31). Les notions d'information et d'entropie sont centrales à cette pensée. Claude Shannon et Warren Weaver, dans *The Mathematical Theory of Communications*, utilisent le terme d'information pour référer aux connaissances « that one does not have about what is coming next in a sequence of symbols » (Broadhurst et Darnell, 2007, p. 446). Ainsi, si l'information relève de la formation des séquences et des symboles, que la connaissance est associée à la capacité de contrôler et de prévoir ces séquences d'informations, alors l'entropie (le désordre) est directement liée à leur manque de prédictibilité (Broadhurst et Darnell, 2007). La prédictibilité de la communication selon le modèle cybernétique relève donc de la capacité du sociologue à être capable de déterminer les champs de possibilité dans l'action humaine. Ces champs, selon Wiener, ne sont pas infinis et le contrôle de l'information vise à établir et à contrôler le spectre des possibilités :

> [...] we devote much of the mathematics to discussions involving the infinite, but these discussions and their accompanying proofs are not infinite in fact. No admissible proof involves more than a finite number of stages. [...] A proof represents a logical process which has come to a definite conclusion in a finite numbers of stages (Wiener, 1965, p. 125-126).

La communication est donc posée comme un mécanisme central de régulation essentiel à l'organisation sociétaire. Voilà pourquoi, selon Céline Lafontaine, « la représentation cybernétique de la communication est circulaire et sans fin. De simples "moyens", l'information devient avec la cybernétique, une véritable fin en soi » (Lafontaine, 2004 p. 46).

Trois aspects inhérents à la pensée cybernétique sont importants à mentionner vu leur influence sur les modes de gouvernances contemporains. La rationalité du système est le premier aspect à soulever. Wiener étant mathématicien de formation, le discours entourant la pensée cybernétique se fonde sur la capacité de transposer les communications humaines en données mathématiques et d'ainsi pouvoir coder l'information sans biais idéologiques. Ensuite, si le contrôle total de l'information est synonyme de paix sociale, d'absence d'antagonisme politique et de désordre, alors le système doit pouvoir avoir accès à une vérité supposément universelle, objective. Au lendemain de la Déclaration universelle des Droits de l'Homme, de la Deuxième Guerre mondiale, et à la veille d'une hégémonie néolibérale, cette conception s'avère tout à fait cohérente avec son contexte sociohistorique. L'entropie est donc nécessairement associée à l'irrationalité, à l'incapacité de faire partie du système, nécessitant de ce fait d'être combattue, afin d'éventuellement être contrôlée, intégrée. Finalement, il est nécessaire de soulever l'autoréférentialité du système cybernétique. Sur la base de la pensée de de Certeau, il serait correct de l'associer à son apogée à l'exercice d'un pouvoir stratégique sans friction, sans mouvements tactiques dans son champ de vision.

2.1.1.2 Le système-monde

Le système-monde a de nombreux points en commun avec la pensée cybernétique. Effectivement, il amène un mode de gestion en apparence non idéologique : où le symbolique est substitué par la technique et par ses rapports processuels (Mondoux,

2009). Ainsi, le discours mis de l'avant par le système-monde prône une rationalité, une neutralité des modes de gouvernance (Freitag, 2007) et se définit ainsi comme le « Réel » (Žižek, 2002). Il s'agit donc d'un discours dont la légitimité est avant tout ancrée dans des rapports processuels. À ce titre, « les concepts de communication et d'information subissent [...] dans le champ des nouvelles technologies informatiques, une mutation radicale de leur sens : les réalités qu'ils désignent spécifiquement ne sont plus d'ordre *symbolique et culturel*, mais *technique* et *opérationnel* » (Freitag, 2003, p. 280).

Dans cet ordre d'idées, si la technique engendre une dynamique en apparence non idéologique, et qui se redouble sur elle-même (autoréférentialité), alors elle impose par la même occasion les limites du système en transformant les formations sociohistoriques en catégories supposément ontologiques :

> Opérationnel, autoréférentiel et totalisant est ainsi créé un système technicien (Ellul, 1977) qui est ainsi non pas représenté comme une production symbolique (discours social dominant), mais bien comme une ontologie en soi, un monde fermé (Edwards, 1996), ou un système-monde (Mondoux, 2007). Ainsi, nous ne sommes plus en société, mais bien dans un système; on ne dit plus capitalisme, mais économie, la base du social est formée non pas de citoyens, mais de consommateurs... (Mondoux, 2011, p. 55).

Ainsi, le système-monde ne reconnaît aucune extériorité, car en reconnaître une invaliderait la prétention d'incarner un monde en soi, c'est-à-dire le « Réel » précédemment invoqué : « De ceci découle la nécessité de fonder les processus de socialisation (l'intégration au système-monde) sur la base de l'impossibilité même d'être en rapport d'extériorité face au système » (Mondoux, 2011, p. 55).

2.1.2 Le politique

Pour faire suite à ces réflexions, nous verrons comment le système-monde (où la rationalité technique permet à la fois d'induire et de légitimer des pratiques de

gouvernance) s'inscrit dans une idéologie néolibérale (l'idéologie relevant ici, entres autres, des valeurs portées dans les pratiques de gouvernance) - permettant ainsi de conceptualiser l'environnement stratégique (idéologie et pratique de gouvernance) dans lequel prennent part les mobilisations hacktivistes.

De cette manière, l'objectif des prochains paragraphes est de rendre compte des stratégies discursives mises de l'avant dans cet environnement stratégique néolibéral en se questionnant sur les valeurs portées par les objets techniques. Cela permettra ensuite de comprendre dans quelle mesure les pratiques hacktivistes relèvent d'une extériorité à ce système-monde en transgressant certains codes désormais promus comme universels et ontologiques.

2.1.2.1 Une hégémonie néolibérale

L'idéologie néolibérale, selon David Harvey, construit son centre de légitimité autour de l'échec des autres systèmes politiques[16] et par la valorisation des libertés individuelles pouvant être atteintes par la liberté des marchés. Il décrit effectivement comment les concepts de liberté individuelle et l'individualisme inhérents au néolibéralisme sont mobilisés dans le discours idéologique afin de renforcir la liberté des marchés et la propriété privée :

> By capturing ideals of individual freedom and turning them against the interventionist and regulatory practices of the state, [...] [n]eoliberalism [...] practical strategy [...] emphasized [on] the liberty of consumer choice, not only with respect to particular products but also with respect to lifestyles, modes of expression, and a wide range of cultural practices. Neoliberalization required both politically and economically the construction of neoliberal market-based populist culture of differantiated consumerism and individual libertarianism (Harvey, 2005, p. 42)

[16] Tel que l'a supporté, entre autre, le slogan politique « There Is No Alternative » (TINA) de Margaret Thatcher.

La liberté et l'émancipation individuelles sont donc comprises à travers une économie politique où le rôle de l'État est de mettre en place des dispositifs légaux, policiers et militaires nécessaires pour assurer le bon fonctionnement des marchés et pour protéger la propriété privée. Les libertés personnelles et de marché dans un monde globalisé sont donc au fondement identitaire de l'idéologie et la protection de ces valeurs, désormais défendues comme étant universelles, assure sa légitimation. Ainsi, comme le note Feenberg, le discours néolibéral « relève de l'efficacité plutôt que de la volonté du peuple, ou plutôt l'efficacité est la volonté du peuple dans les sociétés modernes vouées avant tout à la prospérité matérielle » (Feenberg, 2004, p. 110). Ces valeurs sont ainsi intrinsèquement liées dans les discours politiques et économiques actuels. Les processus de production sont donc à la fois placés au cœur des fondements idéologiques du néolibéralisme et deviennent également un mode de légitimation de celui-ci.

2.1.2.2 Une ontologie sociale

Ainsi, si les structures sur lesquelles est soutenue l'hégémonie néolibérale favorisent le renforcement de la propriété intellectuelle, des intérêts corporatifs (la liberté du marché) et de la propriété privée, alors l'architecture et la gouvernance du cyberespace protègent ces valeurs par des dispositifs à la fois techniques et légaux (Lessig, 2003) qui défendent les réseaux comme fonctionnant de manière rationnelle, neutre et objective. Les valeurs qu'il supporte sont donc posées comme quelque chose de *naturel*, d'« ontologique ».

Dans cette mesure, Nissenbaum mobilise le concept d'ontologie sociale: « According to Searle, it is useful to posit a social ontology, including social entities and facts, in addition to a natural ontology of natural entities and facts. A social ontology [is] [...]

defined by conventions, practices, and institutions of social life » (Nissenbaum, 2004, p. 211). Cette ontologie sociale est indubitablement liée à la gouvernance dans un système-monde (Mondoux, 2007), qui a comme dimension constitutive l'impossibilité de se trouver en son extérieur (se positionner et être reconnu en tant qu'adversité politique antagoniste), c'est-à-dire de ne pas respecter les valeurs ontologiques.

2.1.2.3 L'effacement du politique

De cette manière, en signifiant l'environnement stratégique inhérent au néolibéralisme et en reconnaissant son caractère hégémonique, la critique de Chantal Mouffe (Mouffe, 2007) prend tout son sens. La rationalité technique (Feenberg, 2004) mise de l'avant par le discours du système-monde doublé de ses mécanismes de régulation et de légitimation marque sa prétention d'incarner un monde en soi, puis de renier toute extériorité, c'est-à-dire toute adversité antagoniste.

À cet effet, Mouffe soutient la thèse selon laquelle « le » politique[17] serait évacué des relations politiques contemporaines. Elle oppose le concept « du » politique à celui de « la » politique[18]. Effectivement, « la » politique relève de l'opérationnalisation des politiques à l'intérieur d'un même système idéologique (lois, politiques publiques, etc.). « Le » politique, quant à lui, relève directement du symbolique (Žižek, 2002), des discours servant à construire une réalité (Foucault, 1978) et donc, dans une perspective plus globale, de l'idéologie. Selon Mouffe, tous les débats politiques actuels prennent racine dans le même terrain idéologique. Les adversaires politiques, même s'ils sont en désaccord entre eux, légitiment à tout le moins la structure dans laquelle s'inscrivent leurs débats et partagent les mêmes primats de base, la même identité, les mêmes valeurs, les mêmes codes. Comme noté précédemment,

[17] En anglais : « the political »
[18] En anglais : « the politics »

l'adversité antagoniste tend ainsi, dans le discours néolibéral actuel, à être intégrée en tant qu'adversité agoniste ou à être criminalisée (extériorité).

2.1.2.4 Le hacker

Dans cet ordre d'idées, Helen Nissenbaum soutient dans son article *« The Contested Ontology of Cyberspace »* que la mutation de l'image des *hackers* (de héros à criminel) est due, bien entendu, à un élargissement des répertoires d'action du *hacking*, mais est d'abord causée par les profonds changements structurels du cyberespace et des valeurs qui composent sa structure technique. Ainsi, dans le système-monde, les *hackers* défient les normes et valeurs dites universelles qui composent le cyberespace en contournant les lois sur la propriété intellectuelle et en entrant illicitement dans un système. À ce titre, « the status of hackers in the social ontology of cyberspace is agents who willfully defy the rules as adulteres are to mariage, thieves to property, so hackers are to the the set of interlinked institutions that have colonized the online world » (Nissenbaum, 2004, p. 203). La simple association sémantique entre le *hacker* et le pirate est révélatrice en soi. Alors que le terme *hacker* était utilisé avec fierté au cours des années 1950 pour décrire des actes d'ingéniosité technique, il est désormais associé à la piraterie – l'un des premiers crimes reconnus dans la juridiction internationale — informatique, au criminel.

2.1.3 Conclusion partielle

À la lumière des théories et concepts mis de l'avant au cours des dernières pages, cette conclusion partielle visera à rallier brièvement ces concepts afin de dégager la manière dont se définit le système-monde et les modes de légitimation de son environnement stratégique. Il sera finalement question de poser ce cadre dans le contexte particulier qui nous intéresse, c'est-à-dire dans la gouvernance TIC.

2.1.3.1 Légitimation

En premier lieu, la manière dont sont légitimés les modes de gouvernance du système-monde relève principalement de la rationalité technique mise de l'avant par les codes et valeurs inhérentes à l'hégémonie néolibérale. La rationalité technique (Feenberg, 2004; Marcuse, 1968) consisterait en « l'utilisation de délégations techniques pour légitimer un système de contrôle hiérarchique en expansion » (Feenberg, 2004, p. 77). Cette légitimation passe par un mode de gestion technocratique et en apparence non idéologique et connecté sur le « Réel » (Žižek, 2002), mais où l'idéologie réside au cœur des processus techniques de production. En entretenant constamment une tension avec les résistances tactiques, la stratégie du système-monde viserait à intégrer dans son environnement les actions tactiques afin d'assurer leur domination.

2.1.3.2 Identité

En deuxième lieu, l'identité du système relève directement d'une association entre les idéaux démocratiques et la théorie d'économie politique néolibérale (Dean, 2009). Effectivement, tel que noté par Harvey (Harvey, 2005), le discours néolibéral encourage l'individu à affirmer sa liberté à travers ses choix de consommation, modes de vie, pratiques culturelles, etc. Ceci se fait en se distanciant du pouvoir régulateur de l'État, qui a comme responsabilité de protéger la liberté des marchés (qui se régulent par la concurrrence) et d'ainsi protéger la démocratie et les droits individuels. Il va donc sans dire que la démocratie, telle que véhiculée dans le contexte actuel, est intrinsèquement liée à la capacité de l'État à protéger la liberté des marchés et la propriété privée, tous deux se portant garants des libertés individuelles. Finalement, si toute identité se construit par rapport à une extériorité (Mouffe, 2005), alors le néolibéralisme se forme autour de valeurs universelles et pose l'extériorité en termes d'immoralité plutôt qu'en termes d'adversité antagoniste (Mouffe, 2005).

2.1.3.3 Gouvernance des TIC

Il importe ensuite de reconnaître comment les valeurs portées dans les discours du système-monde affectent la gouvernance des objets techniques et plus particulièrement celle des TIC. Dans le contexte actuel, où l'appropriation et le détournement des TIC sont marginalisés et criminalisés, le cyberespace serait « colonisé » par les stratégies néolibérales. Effectivement, son architecture et sa gouvernance actuelles protègent et encouragent les intérêts du libre marché (Dean, 2009) en opposition à d'autres valeurs (décentralisation, liberté de l'information, émancipation des communautés, neutralité des réseaux) qui ont été à la base de l'émergence du web (Lessig, 2006). Dans cette mesure, si la gouvernance des objets techniques tend à supporter des discours néolibéraux légitimés par la rationalité des processus techniques et qui ne reconnaissent aucune forme d'adversité politique antagoniste, alors il est cohérent que son mode de fonctionnement tout comme les valeurs qu'elle supporte soient posés en terme d'ontologie sociale (Nissenbaum, 2004 ; Searle, 1980), rattachant solidement les notions de légalité, de moralité et de légitimité.

2.1.3.4 L'individualisme et les résistances au système-monde

En prônant la protection libertés des individuelles à travers la liberté des marchés et en défendant sa légitimité par la rationalité technique et scientifique reliée, le système-monde emploie un mode de gouvernance visant à régner dans la multiplicité. Ce mode de gouvernance se construit en parallèle avec ce qu'André Mondoux qualifie d'hyperindividualisme. L'hyperindividu fait partie intégrante du système-monde et ne travaille généralement pas dans le but de se mobiliser en tant qu'adversité antagoniste. Il cherche effectivement à se distancier de toute autorité. Il est ainsi intégré au système-monde qui lui permet de jouir des outils qui lui donneront

l'impression de se réaliser pleinement, notamment par l'acquisition de droits individuels, par les choix de consommation et, finalement, par la protection de l'intégrité physique des sujets, légitimant de ce fait plusieurs pratiques de surveillance (Mondoux, 2007). Ainsi, la stratégie du système-monde se base sur l'inclusion des subjectivités et sur la transparence de celles-ci, c'est-à-dire sur leur capacité à fournir de l'information rendant la vie sociale plus « prévisible » : « In connection with the effective amount of communal information, one of the most surprising facts about the body politics is its extreme lack of efficient homeostatic processes » (Wiener, 1965, p. 159). Le système-monde, tel qu'énoncé plus tôt, se fonde sur des processus de socialisation (transformation de toute adversité antagoniste en adversité agoniste) et d'inclusion pouvant se rapprocher des rapports de pouvoir induits par la panoptique de Foucault :

> [L]a société a instauré un mode de pouvoir qui ne se fondait pas sur l'exclusion [...] mais sur l'inclusion à l'intérieur d'un système dans lequel chacun devait être localisé, surveillé, observé nuit et jour, dans lequel devait être enchaîné à sa propre identité (Foucault, 1978, p. 465).

Cette dynamique peut également se rattacher au capitalisme communicationnel de Jodi Dean qui soutient que toute résistance au système semble désormais s'opérer en utilisant les codes de ce dernier et en le renforçant par la même occasion. Les mouvements tactiques, qui témoignent de la multiplicité des codes qui coexistent dans un même environnement stratégique, sont surveillés, notamment par données générées par l'utilisation des TIC qui permettent d'identifier rapidement tout comportement perçu comme déviant. De Certeau soutient d'ailleurs que la « rationalité technocratique contemporaine » affaiblit les mouvements tactiques qui se perdent ainsi dans un système global :

> Le système où ils circulent est trop vaste pour les fixer quelque part, mais trop quadrillé pour qu'ils ne puissent jamais lui échapper et s'exiler ailleurs. Il n'y a plus d'ailleurs. De ce fait, le modèle « stratégique » mue lui aussi comme perdu dans sa réussite : il reposait sur la définition d'un « propre » distinct du reste : il devient le tout (de Certeau, 1990, p. 65-66)

Dans cette mesure, il devient intéressant de se questionner sur les formes que prennent les mouvements sociaux dans ce contexte. S'il est toujours juste d'affirmer que l'usage des technologies dans les pratiques de *hacking* peut être qualifié de tactique - vu l'isolement et l'individualité des individus s'adonnant à ces pratiques (Levy, 1985) - le hacktivisme, de par son caractère populaire, tend à rendre collectifs (et donc visibles) ces usages tactiques des technologies numériques dans un système qui tend à désorbiter et à rendre invisibles ses tensions et ses oppositions. Ces relations antagonistes font naître, à travers leurs discours, des rapports de pouvoir. Ces rapports deviennent visibles alors qu'un des discours vise à qualifier des mobilisations de violentes, voire de cyberterroristes, alors que l'autre cadre ces protestations comme étant légitimes. Ils démontrent alors les débuts de ce que Foucault qualifie « d'affrontement des stratégies » (Foucault, 1978).

2.2 Usage tactique et affrontement des stratégies

Cette section se penchera spécifiquement sur les liens qu'entretiennent les pratiques hacktivistes avec les mouvements sociaux. Tel que noté précédemment, le hacktivisme peut être compris comme un prolongement des mouvements sociaux dans le numérique. Ces tactiques représentent une innovation dans les répertoires d'actions activistes tout en faisant émerger de nouveaux enjeux de mobilisations qui sont, pour la plupart, liées à la gouvernance des TIC. Cette partie du cadre théorique étudiera dans quelle mesure les pratiques hacktivistes s'inscrivent dans un prolongement des mouvements sociaux, quelles sont les principales problématiques rattachées à ces pratiques de militance et, finalement, à dans quelle mesure elles apparaissent comme des politiques contentieuses (Tarrow, 2010).

2.2.1 « Mass Virtual Direct Action »

Le Mass Virtual Direct Action (MVDA) est une manière de conceptualiser les pratiques de militance en ligne. Le MVDA fait référence aux mobilisations de masse dans un environnement virtuel ayant comme objectif de mener une action directe envers des adversaires politiques. En ce sens « elle prolonge et complique le "Non Violent Direct Action" (NVDA) en transposant les notions de violence et d'action politique dans le cyberespace, occasionnant de ce fait un changement de paradigmes » (Traduction libre : Jordan, 2004, Empl.[19] 1710). Chacune des composantes du MVDA, c'est-à-dire les notions de « masse », de « virtuel » et « d'action directe » seront abordées dans cette partie du cadre théorique. Il sera également question de voir comment chacune de ces composantes rendent problématique l'identification et la légitimation de mobilisations hacktivistes.

2.2.1.1 La masse

La notion de masse relève de la participation d'un grand nombre de militants à une mobilisation. Selon Jordan et Taylor, la masse est nécessaire autant à la légitimation d'un mouvement qu'à la formation d'une identité commune, c'est-à-dire à l'identification du « nous » et du « eux » de Chantal Mouffe.

En premier lieu, le MVDA pose un problème dans la mesure où la « masse » d'individus participant à une mobilisation est plus difficile à reconnaître et peut aisément être confondue avec la mobilisation d'une masse d'information : « [t]he 'mass' [...] cannot be the mass generation of packets[20] of information through automation, something so easily done in the immaterial world of cyberspace. Rather,

---

[19] L'abbréviation « Empl. » est utilisée pour le terme *emplacement.* Ce terme fait office de pagination dans les livres électroniques.

[20] Voir glossaire

it must be the force of many people, embodied in the offline world that gives mass action legitimacy and force » (Jordan et Taylor, 2004, Empl. 2377). Il est ainsi difficile d'assurer la légitimité d'une action en ligne puisque celle-ci peut autant relever du choix d'un grand nombre de personnes de manifester, que d'être une démonstration de la virtuosité technique d'un individu. En prenant en exemple la tactique des actions par déni de service, il est possible de mettre un site hors-ligne en mobilisant un certain nombre de militants (dépendant de la résilience de la page web) tout comme il est possible d'impliquer, à l'aide de logiciels malicieux, des ordinateurs-zombies[21] dans un botnet[22] qui les contrôle à distance afin de mener ladite action. Dans les deux cas, le résultat est le même ; pourtant le deuxième ne répondrait pas au critère de légitimité émis par Jordan et Taylor.

En deuxième lieu, les mobilisations doivent avoir une portée symbolique dépassant la simple réussite de l'acte technique. Celle-ci relève de la notion de masse, car elle rend compte d'une légitimité acquise par la participation massive de militants ainsi que par sa capacité de diffuser et de véhiculer un message politique à l'extérieur du groupe d'activistes. Bref, la portée symbolique d'une mobilisation est grandement liée à la légitimité de celle-ci et sa réussite doit avant tout être évaluée en fonction des critères de rayonnement dans l'espace public et de sa capacité à mobiliser de nouveaux activistes dans des mobilisations futures. Dans un groupe hacktiviste, cette capacité à mobiliser des masses extérieures au mouvement peut s'avérer difficile vu la nature technique des répertoires d'actions utilisés, ceux-ci demandant une connaissance minimale, parfois même importante, des TIC.

Finalement, la participation massive relève de la capacité d'un mouvement à se construire une identité par rapport à l'Autre (Mouffe, 2005). Jordan note que les mobilisations en ligne peuvent être un obstacle à la construction de ces rapports : « It

[21] Voir glossaire
[22] Voir glossaire

is impossible to miss the message and impossible for protestors to miss each other and the feeling of solidarity in the street, while in cyberspace, packets of information flowing across the Net, are simply packets of information » (Jordan, 2004, Empl. 1767). De cette manière, la masse participative dans le MVDA doit également servir à créer une identité commune malgré le caractère abstrait de la circulation d'information dans les espaces numériques. Ce critère de construction identitaire est lié à la création et au rayonnement d'une esthétique et d'une identité commune permettant aux hacktivistes ainsi qu'à la population « extérieure » au mouvement à associer les mobilisations ainsi que le groupe à des enjeux politiques.

2.2.1.2 Le virtuel

La deuxième notion est le « virtuel ». Alors que le MVDA semble s'inscrire dans une continuité du NVDA, les auteurs posent clairement que ce n'est pas parce qu'une action est exercée en ligne qu'elle est nécessairement non violente; les formes de violence prenant place dans le cyberespace pouvant autant être de nature psychologique ou physique. Il s'agit donc de voir dans quelle mesure les principes inhérents au NVDA peuvent être appliqués au MVDA. Pour ce faire, Jordan se rattache à la théorisation de la désobéissance civile par Gandhi et Thoreau. Alors que la *satyaghara* vise à induire le changement social en confrontant l'adversaire avec la supériorité morale des activistes, la désobéissance civile de Thoreau vise à arrêter par l'action directe ce qui est perçu comme immoral. La désobéissance civile par l'action directe, telle que théorisée par Thoreau, a donné lieu à un glissement de paradigme relié à la légitimité de l'usage de la violence dans des mobilisations :

> Some mouvements gradually minimzed debates around the morality of non-violence in favour of its efficacity. In particular, violence against property has become accepted as a component of direct actions, whether than it is raiding a construction office and destroying its computers or, as happened in 2001, torching the four-wheel-drives in an American 'sport utility vehicule' dealership because such vehicules are environmentally destructive (Jordan, 2004, Empl. 933).

Si des actes pouvant être qualifiés de violents sont désormais perçus comme légitimes dans le cadre d'actes de désobéissance civile, il s'agit donc de voir comment cette violence est identifiée et potentiellement légitimée à travers les mobilisations hacktivistes. Il s'agit donc de repenser la notion de violence virtuelle comme étant, en premier lieu, un construit discursif et puis, comme étant reliée aux codes transgressés par les militants (Jordan, 2004). Effectivement, plusieurs acteurs corporatifs et gouvernementaux soutiennent que la violence en ligne peut être exercée envers la propriété privée (Costanza-Chock, 2003) par le vol ou la destruction de données, par la fraude électronique, ou par l'altération d'un système informatique menant, dans le cas des actions par déni de service, à des pertes financières.

2.2.1.3 L'action directe

La dernière notion, la « Direct Action », réfère à la manière dont une mobilisation peut restreindre un adversaire. Le MVDA accorde une grande importance à la dimension symbolique d'un acte de militance, c'est-à-dire que celle-ci doit à la fois restreindre les activités de l'adversaire jugées inacceptables, mais doit également avoir une portée symbolique visant à attirer l'attention des médias et de la population sur une série d'enjeux. Il est donc nécessaire de tenir compte de deux dimensions principales à l'action directe : ses répercussions directes sur lesdites activités de l'adversaire puis des finalités, c'est-à-dire à la manière dont elles permettent l'atteinte de certains objectifs spécifiques ou globaux.

À cet effet, Sasha Costanza-Chock (Costanza-Chock, 2003) a conceptualisé dans son article « Mapping the Repertoire of Electronic Contention » trois types de finalités dans les répertoires d'actions militantes : les finalités reliées à la « mobilisation », à la « politique » et au « culturel ». Il est important de mentionner que ces trois finalités sont conceptuellement séparées qu'à des fins analytiques. Effectivement, une même

mobilisation peut faire appel à de nombreuses tactiques qui ont chacune différentes finalités. En premier lieu, les fins liées à la mobilisation visent, bien entendu, à communiquer un message politique afin d'attirer une masse et de mobiliser des gens à l'extérieur du groupe. Les tactiques pouvant s'y attacher sont l'envoi massif de courriel et l'utilisation tactique des médias sociaux. En deuxième lieu, les fins dites politiques sont liées à des changements de politiques et peuvent de ce fait être associées à des tactiques de lobbying électronique ainsi qu'à des campagnes d'envoi massif de courriels et de fax à des institutions ciblées. Finalement, les finalités culturelles visent un changement dans les « social norms, behaviors, and ways of thinking among a public that extends beyond movement constituents of beneficiaries » (Staggenborg, 1995, p. 341). Il sera abordé dans la prochaine section que les finalités culturelles sont plus aisément associées à des tactiques transgressives.

2.2.2 La transgression

La transgression dans les mobilisations hacktivistes doit être comprise comme une manière de défier les codes établis par le système. La notion de transgression sera abordée premièrement en lien avec l'étude des mouvements sociaux, en l'associant à ce que Sidney Tarrow qualifie de « contentious politics » (Tarrow, 2010). Il sera ensuite question de voir comment elle peut se manifester dans les objectifs politiques d'une mobilisation – en se posant à l'opposé de mobilisations dites « réformistes » — dans les actions techniques de celles-ci ainsi que dans l'esthétisme et l'organisation d'un groupe militant.

2.2.2.1 La transgression et les politiques contentieuses

Selon Tarrow (2010), l'action collective devient contentieuse quand un groupe de personnes n'ayant pas accès aux institutions législatives et exécutives agissent au nom de valeurs nouvelles et d'une manière qui défie les codes établis. Il différencie

un collectif contentieux à un mouvement contentieux. Le collectif sert de précurseur au mouvement qui s'avère beaucoup plus prêt à confronter des adversaires plus puissants par leur manière de « build organizations, elaborate ideologies, and socialize and mobilize constituencies » (Tarrow, 2010, Empl. 508). Moins organisé qu'un mouvement, un collectif contentieux jette néanmoins les bases permettant l'émergence d'un mouvement social et peut s'adonner à des pratiques politiques transgressives. Le hacktivisme est compris comme un collectif contentieux et non comme un mouvement social.

Selon Jordan, la transgression dans les collectifs contentieux apparaît dans l'« identification of problems with at least one social institutions or structure of such magnitude that they cannot be solved from within that institution or structure » (Jordan, 2002, Empl. 500). Il est important de noter qu'un groupe peut être transgressif sans s'opposer à l'ensemble du système présent. Il peut aisément cibler un domaine d'action, une série de codes ou des institutions spécifiques sans nécessairement se poser dans un rapport transgressif total: « [transgression] may also operate on two registers. At one level, they may demand changes from existing social institutions and thereby accept, in some sense, the legitimacy of thoses institutions, while at another level, they may seek the entire reconstruction of social systems » (Jordan, 2002, Empl. 533). Toute action contentieuse cible donc les normes, valeurs et éthiques associées à la transgression des codes.

2.2.2.2 Transgression et réforme

Dans un spectre de militance politique, Jordan oppose la notion de réforme politique à celle de la transgression. La réforme politique induirait des changements à finalité politique (Costanza-Chock, 2003). Ces protestations légitiment donc *de facto* le système en place et leur finalité ne peut être rencontrée qu'à l'intérieur de ce dernier. Les actes de transgressions dans les politiques contentieuses visent, quant à eux, des

finalités culturelles, c'est-à-dire le développement de nouvelles valeurs, principes éthiques, etc. Tel que noté par Jordan, les normes du futur ne peuvent que découler de la transgression puisque la transgression permet de dépasser les moyens usuels de discuter et de régler des conflits sociaux :

> If transgression, in the context of popular political activism, is the contradiction of existing social structures, institutions and ethics. [...] The opposite end of transgression, on the continuum of political activism, always reinforces what exists ; it reforms, but does not change. (Jordan, 2002, Empl. 489)

De cette manière, la transgression dans les politiques contentieuses peut être rattachée à l'adversité antagoniste de Mouffe, alors que la réforme peut être associée à l'adversité agoniste. Effectivement, si une adversité politique antagoniste, selon Mouffe, ne légitime pas les codes, les normes ou les institutions en place, alors les actes transgressifs se posent en opposition à ces structures, institutions et normes (Jordan, 2002; Tarrow, 2010). Elle expose en ce sens les limites du système-monde, elle crée un rapport à l'extériorité en posant de normes nouvelles ou en défendant des principes controversés. La réforme, tout comme l'adversité agoniste, légitime le système en place et expose des demandes qui peuvent être satisfaites à l'intérieur de celui-ci, faisant ainsi partie intégrante du système.

2.2.2.3 Transgression et outils de mobilisation

Si, dans la transgression, les demandes faites ne peuvent être résolues à l'intérieur du système en place, alors il est logique que celle-ci soit reliée à des tactiques dites perturbatrices (Costanza-Chock, 2003). Effectivement, « for movements seeking transgression, being restrained within approved avenues can be unacceptable » (Jordan, 2002, Empl. 846). L'usage détourné des technologies numériques à des fins de militance correspond efficacement à cette vision des tactiques perturbatrices et rattachées à la transgression. Le hacktiviste défie vraisemblablement les codes

techniques portés par l'architecture des TIC pour contraindre un adversaire en exposant des demandes qui ne peuvent être satisfaites dans le contexte politique.

Dans cette mesure, il est possible de comprendre les collectifs contentieux *hacktivistes* comme amorçant un affrontement de stratégies. Effectivement, puisque le système-monde ne reconnaît aucune extériorité et tend à cadrer l'adversité antagoniste comme une forme criminalité en la démunissant, entre autres, par des processus discursifs de son caractère politique. Cela permet au système-monde d'intégrer les pratiques transgressives en les posant comme des ennemis à l'ordre en place, à la paix sociale, lui permettant ainsi de renforcer son pouvoir

CHAPITRE 3 : MÉTHODOLOGIE

Une analyse critique du discours d'une mobilisation hacktiviste a été menée autour du cas de l'*Operation : Payback* du collectif Anonymous, ayant pris place entre les mois de septembre 2010 et février 2011. Le but est ici d'étudier la manière dont sont cadrées les mobilisations hacktivistes et de voir comment ce cadrage témoigne de rapports de pouvoir. Il a ainsi été question de relever et de comparer les discours mis de l'avant par les médias et par les hacktivistes afin d'identifier :

1) la manière dont est identifié le collectif Anonymous à travers les discours des médias de masse américains et celles des militants;

2) la manière dont est décrite l'*Operation : Payback* dans les discours des médias de masse américains et celles des militants;

3) la manière dont les revendications politiques et pratiques techniques du collectif Anonymous remettent en question les codes techniques de l'environnement stratégique néolibéral;

4) les enjeux sociopolitiques, éthiques, sécuritaires, économiques et légaux utilisés dans les discours de ces médias et dans celui des hacktivistes afin de supporter leurs cadrages respectifs des mobilisations.

3.1 Type de devis de recherche : recherche qualitative inductive

Le type de devis de recherche choisi pour mener cette étude est une recherche qualitative inductive. Celle-ci « consiste à donner priorité aux données, à l'expérience vécue, au terrain pour ensuite avoir recours aux savoirs constitués dans un processus de construction de connaissance » (Luckerhoff, 2012). Il s'agit d'explorer en profondeur un cas de recherche pour en dégager des résultats pouvant être attribués à une majorité de luttes de cadrage entourant les pratiques hacktivistes.

Tel que mentionné dans la problématique de recherche, l'étude se situe à l'intersection de trois corpus de littérature. Le premier corpus traite du cadrage des *hackers* par les médias depuis 1950, le second est relié aux études ethnographiques portant sur le collectif Anonymous et le dernier soulève les travaux entrepris dans l'optique d'analyser la légitimité des actes de désobéissance civile électronique depuis 1990. En ayant pour objectif de combler un vide dans la littérature existante, l'étude du cadrage des pratiques hacktivistes du collectif Anonymous s'avère rallier ces trois corpus sous l'angle de l'analyse discursive. Effectivement, la construction de l'image des hacktivistes dans l'imaginaire public par des processus discursifs aborde plusieurs aspects exposés par les trois corpus de littérature en mettant cependant l'emphase sur les rapports de pouvoir engendrés par l'usage tactique des TIC dans un contexte de militance politique. De cette manière, en situant la problématique dans un contexte historique plus large – celui des cadrages du *hacking* depuis 1950 — et en abordant une nouvelle dimension aux pratiques de *hacking* ainsi qu'aux pratiques de militance politique – c'est-à-dire la désobéissance civile électronique —, la recherche vise à refléter une tendance plus globale dans le cadrage des pratiques hacktivistes.

3.2 Étude de cas : Anonymous et l'Operation : Payback

3.2.1 L'*Operation : Payback*

Operation : Payback a pris place entre les mois de septembre 2010 et janvier 2011 et a sommairement consisté en une série de micromobilisations (Coleman, 2014) en premier temps, contre les industries du divertissement. Cette opération a débuté alors qu'une compagnie indienne, Aiplex Software, a mené une série d'actions par déni de service contre le site « The Pirate Bay » afin que les activités de ce dernier cessent. Une fois la nouvelle arrivée sur la plateforme/b/de 4chan, plusieurs membres du collectif Anonymous se sont mobilisés afin de contre-attaquer. Ainsi, Anonymous a rapidement élargi les enjeux liés à la problématique en orchestrant une série de mobilisations contre les mesures restrictives mises de l'avant par les lois relatives à la protection de la propriété intellectuelle et appliquées par de nombreux acteurs corporatifs et gouvernementaux. Lors de ces mobilisations, les principales cibles ont été des cabinets d'avocats (ACS : Law, Davenport Lyons et Grubb & Weaver), des organisations et associations dévouées à la protection des lois sur la propriété intellectuelle (Australian pro-copyright organization, Recording Industry Association of America, Motion Picture Association of America, etc.) ainsi que des musiciens et des militants pro-copyright (Gene Simmons, par exemple).

Au mois de décembre 2010, suite à la publication de plusieurs centaines de milliers de documents confidentiels relatifs aux guerres en Irak, en Afghanistan ainsi que sur la prison de Guantanamo (Greenberg, 2013) par Chelsea Manning[23], PayPal, Visa et MasterCard ont décidé de retirer leurs services à l'organisme controversé Wikileaks. La raison invoquée par ces compagnies est un « non-respect des conditions

[23] Chelsea Elizabeth Manning, née Bradley Edwards Manning, était, lors de la publication desdits documents, de sexe masculin et connu sous le titre de soldat Manning. Elle a annoncé dans un communiqué de presse, la journée suivant la fin de son procès, qu'elle était en période de transition sexuelle et souhaitait désormais que toute référence faite à son égard soit au féminin (The Guardian, 2013).

d'utilisation ». Cette partie de *Operation : Payback,* appelée *Operation Avenge Assange,* a ciblé différents organismes gouvernementaux et personnalités publiques (tels que Sarah Palin s'étant manifestée comme radicalement opposée à Wikileaks).

Ces actions ont résulté en l'interruption de service ou, du moins, le ralentissement significatif de la majorité des sites ciblés (MPAA, Aiplex, RIAA, British Pornographic Industry, PayPal, Mastercard, Visa, etc.) pour une durée moyenne de quelques heures (Olson, 2012). L'opération a manifestement été très controversée et a amené les gestionnaires de réseaux sociaux tels que Facebook et Twitter à fermer les comptes liés aux opérations d'Anonymous pour cause de non-respect des conditions d'utilisation, rendant de ce fait la communication tactique plus compliquée entre les militants. Au cours de l'année 2011, plusieurs mandats de perquisition ont été lancés par le FBI, menant à l'arrestation de plus de 25 hacktivistes. Finalement, l'*Operation: Payback* a connu une très grande couverture médiatique, tant pendant les mobilisations que pendant l'arrestation des hacktivistes. Bref, elle a mis en lumière dans l'espace public des débats relatifs à la propriété intellectuelle, à la censure sur l'Internet ainsi que sur l'usage des TIC dans un contexte de militance.

3.2.2 Tactiques techniques : Actions par déni de service

Le logiciel utilisé pour mener les actions par déni de service, le *Low Orbit Ion Canon*[24] (LOIC), est un logiciel à code source ouvert[25] permettant d'envoyer des « paquets d'informations » vers un site web préalablement ciblé. Cette action peut se faire soit de manière manuelle soit en joignant son ordinateur à un *botnet* volontairement. Le mode manuel nécessite que le hacktiviste sélectionne lui-même le site, le débit d'envoi des paquets d'information ainsi que le moment où débutent et

[24] Voir glossaire
[25] Voir glossaire

cessent les actions tandis que pour joindre un botnet de manière volontaire[26], le hacktiviste donne son adresse IP[27] à un ordinateur central qui contrôle par la suite l'ensemble des aspects des actions. Les actions par déni de services peuvent cependant également mobiliser des botnets non volontaires[28]. Ces botnets sont composés d'ordinateurs infectés d'un vers ou d'un virus, nommés ordinateurs zombies et sont contrôlés par un botmaster[29] qui dirige les opérations à distance. Dans le cas de *Operation : Payback,* l'utilisation de botnets involontaires a permis aux hacktivistes de rendre inaccessibles des sites d'entreprises internationales, techniquement configurés pour recevoir un très grand achalandage. Dans les mobilisations entourant *l'Operation : Avange Assange,* environ 90 % de la force de frappe ayant servi à cesser l'activité des sites comme PayPal, serait provenue de botnets mobilisant des ordinateurs non volontaires, contre seulement 10 % provenant des ordinateurs des militants ayant joint les botnets de manière volontaire (Olson, 2012).

Dans la législature américaine, ainsi que dans la majorité des pays du monde, les actions par déni de service sont illégales. Effectivement, aux États-Unis, ces actions entrent sous la législation du « Computer Fraud and Abuse Act » qui empêche toute personne de « knowingly cause the transmission of a program, information code, or command, and as a result of such conduct, intentionally causes damages without authorization to a protected computer » (voir 18 U.S.C. § 1030[a] [5] [A]). Aussi, la section U.S.C.§ 1030(b) de la même loi stipule qu'une action n'a pas besoin d'être techniquement réussie pour être illégale et pour entraîner des poursuites.

---

[26] Voir glossaire
[27] Voir glossaire
[28] Voir glossaire
[29] Voir glossaire

Cependant, tel que noté par Parmy Olson, une journaliste ayant enquêté auprès des groupes d'Anons[30], dès le début de l'Operation : Payback, seulement une faible proportion des hacktivistes impliqués comme participants ou comme dirigeants d'opérations avaient des connaissances informatiques suffisantes pour être capables de lire le code source du logiciel LOIC afin de voir dans quelle mesure ce logiciel protégeait l'adresse IP des ordinateurs des militants. Alors que plusieurs *Anons* écrivaient sur les canaux des IRC que les chances que l'ordinateur d'un hacktiviste soit retracé frôlaient le zéro, un programmeur ayant joint une mobilisation a exploré le code source du logiciel open source pour découvrir que « the big problem was that the application was sending junk traffic directly from users' IP addresses. It did nothing to hide their computer in the network. This meant the people who used LOIC were doing so with their IP addresses exposed, and just asking to get arrested » (Olson, 2012, p. 126). Il n'est donc pas surprenant que le 15 décembre 2010, quelques jours après les premières actions envers PayPal, le département de cybersécurité ait été en mesure de fournir au *Federal Bureau of Investigation* (FBI) une clé USB contenant les mille adresses IP des ordinateurs ayant envoyé la plus grande quantité de paquets d'information. Le FBI a ensuite été en mesure, en faisant appel aux fournisseurs de services Internet (tel que AT&T, par exemple), d'associer les adresses IP aux adresses physiques de ces ordinateurs, menant à l'arrestation aux États-Unis de 14 membres d'Anonymous au mois de janvier 2011. Ces quatorze *Anons* sont désormais connus sous le nom des « PayPal 14 ».

3.2.3 Anonymous

Le choix du collectif Anonymous pour mener une étude de cas portant sur le hacktivisme s'est avéré nécessaire à plusieurs niveaux. Premièrement, tel que relevé

[30] Voir glossaire

plus tôt, Anonymous a émergé de sous-cultures web, telles que le *trolling*, et s'est construit une identité autour de pratiques et de normes qualifiées de transgressives.

Depuis l'opération *Chanology* menée contre l'Église de la Scientologie en 2008, les mobilisations d'Anonymous visent avant tout à attirer l'attention des médias (Coleman, 2012). Bien que toutes les opérations n'aient pas eu le même succès, il n'en reste pas moins que le collectif a su gagner une certaine notoriété. Effectivement, plusieurs ouvrages académiques font la constatation que les symboles associés au collectif sont reconnus et utilisés dans divers contextes et font directement référence aux valeurs prônées par le collectif. Premièrement, l'établissement d'une esthétique commune, d'un logo (homme en complet sans tête), d'un visage commun marquant l'anonymat (le masque de Guy Fawkes) et d'un slogan (« We are Anonymous, We are Legion. We do not forgive. We do not forget. Expect us ») permet aux symboles du collectif d'être présents lors de divers événements hors-lignes (grèves, manifestations et les mouvements Occupy).

Alors que de nombreux organismes militent autour de problématiques semblables (Free Software Foundation, Electronic Frontier Foundation, etc.), ceux-ci travaillent davantage derrière des portes fermées en engageant la population civile de manière restreinte dans les actes de militance (pétitions électroniques, par exemple) tout comme dans leur organisation (Coleman, 2014). Dans cet ordre d'idées, Anonymous favorise la mobilisation populaire et construit son image autour de cette structure inclusive. Cependant, dans un collectif hacktiviste, le fait que plusieurs militants n'aient que très peu de connaissances informatiques crée nécessairement une fissure entre les réels *hackers* et ceux qui sont appelés des *script kiddies* [31]. Un *script kiddy* est quelqu'un « who may hold ambitions to be a black hat hacker and who uses well-known and freely available Web tools, or ''scripts'', to attack networks » (Olson,

[31] Voir glossaire

2012, p. 452). Dans le cas spécifique de l'*Operation : Payback*, l'incapacité de certains hacktivistes à comprendre et à reconnaître que le code source du LOIC ne protégeait nullement les données personnelles présentes sur les ordinateurs impliqués dans l'action ainsi que le manque de connaissances relatives à la protection de l'adresse IP d'un ordinateur durant la mobilisation a mené à l'arrestation de plusieurs *script kiddies* au mois de janvier 2011 – les « vrais » *hackers* ayant été capables de semer les pistes menant à leur ordinateur.

3.3 L'analyse critique foucaldienne du discours

3.3.1 Le discours et la construction de la réalité collective

Dans ses travaux, Foucault associe directement la notion de discours à celle de la construction de la réalité collectif et donc, à l'émergence de rapports de pouvoir. Effectivement, pour Foucault, le discours comme objet d'étude est perçu comme une réalité matérielle et permet la construction de sujets individuels et d'une réalité collective (Foucault, 1978; Lind, 1992; Jäger, 2009) : « [d]iscourses determine the way in which a society interprets reality and organizes further discursive and non-discrusive practices » (Jäger et Maier, 2009, p. 38). En ce sens, les discours forment la conscience individuelle et collective qui détermine ensuite les actions possibles dans un plus grand registre d'actions. En prescrivant quelles actions sont « possibles », le discours s'inscrit dans une logique de gouvernementalité engendrant conséquemment des rapports de pouvoir (Foucault, 1978).

Les rapports de pouvoir véhiculés à travers les discours influencent la manière dont une société interprète la réalité et sont également prolongés dans le concept de ce que Foucault qualifie de dispositif. Les dispositifs sont, en quelque sorte, une *matérialisation des discours* et font référence à « these strategic assemblages [that] are initially formed as responses to crises, problems, or perceived challenges by those

who govern. The apparatus is a response to a specific historical problem » (Raibow et Rose, 1994, p. vii). Cela peut se rapporter, tel qu'établi plus tôt, à la manière dont les TIC représentent une matérialisation des discours néolibéraux. De ce fait, leur usage et leur mode de gouvernance relèvent tous deux du discours et participent à la création d'une réalité auprès de sujets individuels et collectifs.

Nous avons abordé les mobilisations hacktivistes en ce sens: en examinant comment les discours entourant ces mobilisations contribuent à créer une réalité entourant l'image du hacktiviste et en étudiant comment cette dernière s'avère porteuse de rapports de pouvoir relatifs non seulement à la gouvernance du cyberespace, mais aux relations politiques contemporaines dans le système-monde. Bien que Foucault soutienne que des rapports de pouvoir soient induits à la fois dans les discours que dans les dispositifs techniques (i.e. les TIC), pour des raisons de contraintes temporelles, le présent mémoire est uniquement axé sur les rapports de pouvoir portés par les discours relatifs à la construction de l'image du hacktiviste dans le discours des médias de masse américains et dans celui des militants. Cette construction de l'image du hacktiviste reste cependant intrinsèquement liée à l'usage des objets techniques.

3.3.2 Objectifs de l'analyse foucaldienne du discours

Une analyse foucaldienne du discours accorde une grande importance à ce qui est dit à propos du hacktivisme, au contexte rattaché à l'événement discursif et, surtout, à la manière dont le tout est énoncé : « [Critical Discourse Analysis] aims to disentangle the giant milling mass of discourses, to chart what is said in a given society at a given time with regard to its qualitative spectrum (what is said ? How is it said ?) » (Jäger et Maier, 2009, p. 35). Ainsi, le choix d'un sujet doit impérativement être accompagné d'un lieu et d'un temps donné. Cela permet de situer, d'une part, le discours dans son

contexte social et, d'autre part, de remarquer comment ce dernier tend à influencer la construction d'une certaine image des hacktivistes parmi toutes celles possibles.

De manière plus importante, l'analyse proposée est basée sur le principe que tout discours est une construction sociale, le rendant porteur de rapports de pouvoir. En adoptant cette posture, il importe de reconnaître que notre position en tant que chercheurs relève également d'un construit. Elle vise à relever «the means by which discourses makes particular statements seem rational and beyond all dought, even though they are valid only at a certain place and time » (Jäger et Maier, 2009, p. 36). Alors que les discours peuvent avoir la prétention de présenter des faits, de manière objective de représenter des facettes de la réalité, l'analyse critique du discours tente d'isoler le discours pour analyser les contradictions inhérentes à la construction de la réalité à travers des processus discursifs porteurs de rapports de pouvoir.

Bref, l'analyse critique de discours s'opère à travers deux éléments. Le premier est relatif au temps et au contexte dans lequel un discours est émis. Ainsi, la prochaine section abordera l'aspect contextuel amené par Jäger et Maier comme les concepts de dimensions synchroniques et diachroniques du discours. Le second élément est ce que Jäger et Maier qualifient de plan et secteur du discours.

3.3.3 La dimension synchronique du discours

Selon Jäger et Maier, les dimensions synchronique et diachronique du discours sont complémentaires dans la mesure où elles démontrent qu'un discours est le produit de son contexte. La dimension synchronique relève d'un discours pris à un moment particulier et faisant partie d'un contexte plus grand, alors que la dimension diachronique témoigne du contexte historique plus large et regroupe ainsi un assemblage de coupures synchroniques. La recherche proposée s'inscrit dans une analyse synchronique qui « cut through a discourse strand [to] examine a finite

spectrum of what is said and sayable at a particular point in time » (Jäger et Maier, 2009, p. 46). Les discours analysés s'étendent donc dans un spectre temporel allant depuis le mois de septembre 2010 – date des premières actions par déni de services effectuées dans le cadre de l'*Operation : Payback* – jusqu'au mois d'août 2013. Ainsi, il a été possible d'étudier les discours relatifs à cet événement à différents moments clés : aux moments desdites actions par déni de service (septembre 2010 au mois de février 2011), au moment des arrestations des hacktivistes (janvier au mois de juillet 2011) jusqu'au temps présent, où les « PayPal 14 » subissent un procès.

Cependant, si l'événement représente une analyse synchronique du discours, il est tout de même nécessaire de tenir compte du contexte dans lequel s'inscrit cette mobilisation. Ainsi, « [i]n a way, a synchronic cut through discourse strand is always also a diachronic one. This is because each topic has a genesis, a historical a priori. When analysing a topic, the analyst has to keep an eye on the history » (Jäger et Maier, 2009, p. 47). Dans la recherche actuelle, il s'avère donc nécessaire de situer les discours relatifs à *l'Operation : Payback* (dimension synchronique) dans un contexte tenant compte de la construction de l'image des *hackers* depuis leur émergence en 1950 (dimension diachronique); celle-ci étant intrinsèquement liée à la construction de l'image du hacktiviste actuelle.

3.3.4 Les plans et secteurs du discours

Les plans de discours sont caractérisés comme les « social locations from which speaking takes place » (Jäger et Maier, 2009, p. 48). Il est ainsi possible de parler des discours issus des plans juridiques, médiatiques, scientifiques, artistiques, etc. Chaque plan discursif peut ensuite être divisé en secteurs, constituant des facettes plus spécifiques de chaque plan : « A discourse plan consists of various sectors. For example, women's magazines, TV news broadcast and newspaper are different

sectors of the discourse plane of the media » (Jäger, 2009, p. 48). La recherche cible le plan des médias et en compare les discours issus de deux secteurs différents : celui des canaux de nouvelles télévisuelles américaines dont les reportages sont diffusés sur plateforme web ainsi que celui des productions médiatiques (vidéos, images, communiqués de presse) des hacktivistes diffusés sur le web. L'objectif est ici d'établir une tension, une distance ou une proximité, entre les principes légaux ou éthiques mis de l'avant dans les discours.

3.3.4.1 Premier secteur discursif : Les chaînes de nouvelles aux États-Unis

Le choix du secteur discursif des chaînes de nouvelles aux États-Unis a été basé sur deux critères principaux. Le premier critère était celui du rayonnement du média auprès de la population. Ce critère relève de la capacité du discours à être diffusé dans l'espace public. Effectivement, avec la prémisse selon laquelle le discours tend à façonner la perception publique, il est nécessaire, en voulant étudier les rapports de pouvoir entourant la construction de l'image des hacktivistes, d'étudier spécifiquement les diffuseurs de nouvelles ayant le plus de rayonnement auprès de la population. À ce titre, le choix d'étudier les documents médiatiques issus des réseaux de nouvelles télévisuelles est expliqué par le fait que la télévision est le principal média à travers lequel la population américaine se procure des nouvelles d'actualité (Pew Research Group, 2014).

Le deuxième critère relève du lieu géographique où les nouvelles sont produites et diffusées. Dans le cas de la présente recherche, il a été question d'étudier uniquement des documents médiatiques produits et diffusés aux États-Unis. Ce critère est appuyé par la nécessité d'ancrer les normes éthiques, juridiques et morales mises de l'avant dans le discours des médias, dans un même contexte géographique, culturel et juridique. De plus, le cas étudié est largement lié au contexte américain, ne serait-ce que par le fait que PayPal est une entreprise américaine, par la participation de

plusieurs hacktivistes américains dans l'opération, par l'implication du FBI dans les arrestations et les poursuites en cour des « PayPal 14 » dans cette juridiction. Il est à noter que les reportages de chaînes américaines diffusés à l'étranger n'ont pas été sélectionnés.

La sélection spécifique des articles a été faite par rapport à quatre thématiques de critères :

1) Date de publication : Les articles à l'étude doivent impérativement avoir été publiés entre les dates du 15 septembre 2010 (date des premières mobilisations d'Anonymous sous la bannière de l'Operation : Payback) et du 20 août 2013 (dates marquant la fin des arrestations des hacktivistes par le FBI)
2) Le rayonnement des documents médiatiques dans l'espace public : ce critère s'est opérationnalisé dans la sélection des trois chaînes de nouvelles ayant eu les plus grandes cotes d'écoute aux heures de pointe au cours de l'année 2010 : Fox News, CNN et MSNBC (voir la figure A.2 en annexe A) (Pew Research Center, 2014); ainsi que dans la sélection des deux réseaux ayant la plus grande cote d'écoute pour les nouvelles du soir : ABC News et NBC (voir la figure A.3 en annexe A) (Pew Research Center, 2014).
3) Type de document médiatique : Le document médiatique doit être soit un reportage télévisuel diffusé sur les ondes télévisuelles américaines et disponible pour consultation en ligne, ou un article écrit publié sur les pages web des diffuseurs de nouvelles préalablement sélectionnés. Effectivement, les diffuseurs de nouvelles accompagnent souvent les reportages vidéo d'articles écrits. Les nouvelles en ligne sont classées au deuxième rang (après la télévision) dans le palmarès des médias où les Américains se procurent le plus de nouvelles (Pew Research Group, 2014).

4) Contenu des documents médiatiques : Les documents médiatiques doivent aborder de manière relativement exhaustive l'Operation : Payback. Tout article – ou section d'article – doit donc nécessairement allouer un minimum 200 mots à la couverture de l'événement.

Ces critères ont mené à la sélection de 34 documents médiatiques : neuf issus de la chaîne Fox News, onze issus de la chaîne CNN, onze issus du réseau ABC, deux issus de la chaîne MSNBC et deux du réseau NBC. La liste complète des articles et de leurs notices bibliographiques est disponible en annexe B.

3.3.4.2 Second secteur discursif : les productions d'Anonymous

En tenant compte de la nature décentralisée du collectif Anonymous, il n'est pas question d'analyser les discours issus d'une plateforme particulière, mais plutôt de récolter des documents vidéo publiés sur des chaînes YouTube associées au groupe, des communiqués de presse émis par des *Anons* ainsi que des images et textes publiés sur les réseaux sociaux. Le choix de la plateforme YouTube peut être simplement expliqué : la publication de vidéos est d'abord le mode de communication tactique le plus employé par les *Anons* (Coleman, 2014), puis il s'agit du seul réseau social à grand déploiement n'ayant pas retiré les documents médiatiques – Facebook et Twitter ayant suspendu les comptes de l'opération pour cause de « non-respect des conditions d'utilisation ». De cette manière, la sélection des documents s'est opérée à partir de critères similaires à ceux exposés plus haut :

1) Date de publication : Les documents doivent avoir été publiés entre les dates du 15 septembre 2010 et du 20 août 2013.
2) Types de documents médiatiques : Deux types de documents sont à l'étude. Premièrement, des images (c'est-à-dire des documents publiés par les *Anons* en

format JPG, PNG, etc.) dont le contenu peut s'apparenter à des tracts ou à des communiqués de presse constituent une partie du corpus d'analyse. Ce type de communication est grandement utilisé par les membres du collectif. Le deuxième type de document médiatique à l'étude est celui des productions vidéo publiées sur les réseaux sociaux (YouTube, par exemple). Effectivement, les productions vidéo sont utilisées par les membres du collectif Anonymous pour faire des appels à la mobilisation, pour s'adresser à leurs adversaires et pour expliquer les enjeux d'une mobilisation.

3) Contenu des documents médiatiques : Le premier critère est celui selon lequel les documents doivent compter un minimum de 200 mots pour être analysée. Le second vise à ce que tout document à l'étude ait été produit afin d'être diffusé à l'extérieur du collectif. Les documents doivent être des appels à la mobilisation, doivent communiquer les actions à venir ainsi que leurs objectifs. Bref, il ne s'agit pas d'examiner les documents produits de communication tactique, mais bien d'étudier les documents destinés à une diffusion extérieure aux membres mobilisés dans l'opération.
4) Le rayonnement dans l'espace public : La sélection des vidéos à l'étude s'est basée sur le critère du nombre de « vues ». Effectivement, une analyse préliminaire des résultats d'une recherche utilisant les mots-clés « Operation Payback Anonymous » a été faite. En actionnant le filtre permettant de classer en ordre décroissant les résultats de la recherche selon le nombre de vues, nous avons sélectionné les cinq premières vidéos correspondant aux critères précédents. Le nombre de vues de la dernière en liste (25 000) a servi de barème pour la sélection des autres vidéos. Une recherche plus exhaustive, avec différentes variations de mots-clés, a ensuite été menée pour identifier d'autres vidéos. Pour ce qui est des « images », les cinq documents les plus récurrents sur les plateformes « image.google.com », « knowyourmeme.com », « encyclopediadramatica.es » et « wikipedia.org » ont été sélectionnés. Deux

plateformes ont été ciblées soit pour leur capacité à rejoindre un grand public (« images.google.ca » et « wikipedia.org »). Les sites « knowyourmeme.com » et « encyclopediadramatica.es » ont été identifiés premièrement pour avoir répertorié de l'information concernant les mobilisations de l'*Operation : Payback,* puis par la notoriété de ces sites *wiki*[32] — c'est-à-dire de ces sites où le contenu des pages peut être modifié par les utilisateurs — en matière de « sous-cultures » du web.

Ces critères ont mené à la sélection de 9 documents : six vidéos diffusées sur YouTube et trois images. La liste complète des documents ainsi que leurs notices bibliographiques sont disponibles à l'annexe B.

3.3.5 Analyse structurelle du discours

En s'inspirant de la méthode d'analyse critique de discours décrite par Jäger et Maier dans l'article « Theoretical and methodological aspects of Foucauldian critical discourse analysis and dispositive analysis » du livre « Methods of Critical Discourse Analysis », les deux corpus ont été soumis à une analyse opérée en trois temps.

La première étape visait à constituer une liste des documents sélectionnés pour l'analyse. Cette liste devait inclure les notices bibliographiques des documents, leur genre, les principaux sujets qui y étaient traités ainsi que leurs principales caractéristiques. La deuxième étape avait pour objectif de décortiquer chacun des articles de manière à en retirer différents énoncés, différents types d'information. Cela a permis:

---

[32] Voir glossaire

1) De relever les champs lexicaux — ainsi que leur récurrence — utilisés pour traiter des différents sujets abordés dans les documents à l'étude;

2) D'analyser les éléments visuels présentés dans le document, ceux-ci venant souvent appuyer un argument ou un cadrage spécifique;

3) De noter, s'il y a lieu, les articles cités ou reliés aux documents à l'étude. La provenance et la nature des sources utilisées afin de soutenir un argument peuvent effectivement enrichir ou renforcer un certain cadrage.

4) De noter, s'il y a lieu, les intervenants mobilisés dans un article et la manière dont ils sont présentés.

5) De relever les usages de symboles populaires. Pour Jäger et Maier, cela se rattache aux catachrèses qui amplifient le pouvoir du discours : « Catachreses establish connections between statements, links up spheres of experience, bridge contradictions and increase plausibility. » (Jäger et Maier, 2009, p. 48).

La troisième étape rattachait les énoncés relevés dans la section précédente à la fois aux deux noyaux de significations relevés dans le cadre théorique, c'est-à-dire la construction identitaire d'Anonymous ainsi que la légitimité de leurs mobilisations. Il a ensuite été question de voir comment ces deux noyaux de signification ont été rattachés à des enjeux d'ordre politique, éthique, légal, sécuritaire, économique inhérents aux mobilisations hacktivistes de manière à voir comment ces enjeux ont été abordés et avec quelle récurrence. Finalement, nous avons cherché à identifier quels enjeux étaient négligés dans les discours et en quoi cette absence s'avère elle aussi révélatrice.

3.3.5.1 Utilisations du logiciel Nvivo

Le logiciel NVivo a été utilisé afin de pouvoir analyser toutes les données écrites (articles ainsi que les verbatim des reportages vidéo). Le logiciel a été mis à profit afin d'identifier efficacement des fragments de discours et pour les rattacher à des noyaux de signification et à des enjeux identifiés dans la grille ici-bas. Il a ensuite été utilisé pour relever des tendances dans le codage du texte - l'objectif étant de voir quels enjeux ont le plus fréquemment été utilisés et à quelles dimensions et noyaux ils sont le plus souvent associés.

3.3.5.2 Grille d'analyse : L'identité d'Anonymous

Le premier noyau de signification relève de l'identité d'Anonymous en tant que collectif. Les dimensions utilisées pour analyser la représentation du collectif sont : sa capacité d'une mobilisation de masse, son mode organisationnel, la représentation des individus prenant place dans ces mobilisations et, finalement, l'esthétisme et les valeurs qui lui sont associées.

Noyaux	Dimensions	Enjeux	Énoncés du document x	
			Réforme	Transgression
Identité d'Anonymous	Capacité de mobilisation de masses	Politiques		
		Éthique		
		Légal		
		Sécuritaire		
		Économique		
	Organisation	Politique		

		Éthique		
		Légal		
		Sécuritaire		
		Économique		
	Activistes	Politique		
		Éthique		
		Légal		
		Sécuritaire		
		Économique		
	L'esthétisme et valeurs	Politique		
		Éthique		
		Légal		
		Sécuritaire		
		Économique		

0.1 Grille d'analyse : Identité d'Anonymous

La capacité de mobilisation de masse relève de la formation de l'identité d'un groupe militant, à sa capacité à mobiliser des personnes extérieures au groupe. Cet indicateur est lié à la finalité de « mobilisation » exposée par Costanza-Chock et témoigne de la représentation des valeurs fondamentales du collectif ainsi que de la manière dont elles sont véhiculées dans l'espace public (par quels médias, sous quelles formes, etc.)

L'organisation du collectif est directement liée à sa structure interne, ou plutôt à la manière dont cette structure est décrite et potentiellement associée, par son caractère décentralisé et par l'anonymat des hacktivistes, à des pratiques transgressives.

Il s'agit ensuite de voir de quelle manière les activistes prenant place dans les mobilisations sont décrits : comme de virtuoses techniques directement reliés à l'image des *hackers* ou comme des militants possédant peu de connaissances techniques.

L'esthétisme mis de l'avant par le collectif et les images utilisées pour représenter ce dernier est une dimension essentielle à l'analyse de la construction de l'identité du collectif. Effectivement, il permet de mettre de l'avant des codes visuels et des symboles qui sont associés, dans l'imaginaire populaire, à Anonymous.

3.3.5.3 Grille d'analyse : la légitimité

Puisque les mobilisations hacktivistes mobilisent une variété de tactiques, la présente partie de la méthodologie vise à fournir une série d'indicateurs permettant d'analyser le caractère légitime ou illégitime des tactiques.

Légitimité des mobilisations	Nature des actions techniques	Politique		
		Éthique		
		Légal		
		Sécuritaire		
		Économique		
	Finalité des actions	Politique		
		Éthique		
		Légale		
		Sécuritaire		
		Économique		

	Légalité	Politique		
		Éthique		
		Légale		
		Sécuritaire		
		Économique		
	Violence/non-violence	Politique		
		Éthique		
		Légale		
		Sécuritaire		
		Économique		

0.2 Grille d'analyse : Légitimité des mobilisations

La première dimension relève de la manière dont sont décrites les actions techniques du collectif. Il est ensuite question de voir à quelles finalités sont associées ces mobilisations et pratiques techniques, c'est-à-dire si l'objectif global des mobilisations est lié à des objectifs de mobilisation, de changements politiques ou culturels (Costanza-Chock, 2003).

Ensuite l'indicateur de la *légalité* des actions techniques peut également s'avérer intéressant. Effectivement, puisque les mobilisations hacktivistes représentent de nouveaux répertoires d'actions dans le domaine de la militance politique, il est possible que certaines tactiques se situent dans des zones grises de la loi. Dans tous les cas, il est intéressant de voir comment, dans le contexte du système-monde, les notions de légalité et de légitimité sont associées dans les discours à l'étude.

Nous avons ensuite analysé de quelle manière la notion de *violence (*ou de *non-violence)* est mobilisée dans le cyberespace. Cette dimension s'opère à trois niveaux. Le premier niveau relève du cadrage d'une action tactique comme étant de nature violente ou non. Le deuxième niveau permet d'identifier le type de violence associé à la tactique (physique, psychologique, envers la propriété privée). Le troisième, s'il y a lieu, est lié à la notion de légitimation d'un acte potentiellement violent, mobilisant de ce fait des principes légaux, éthiques ou moraux.

Ensuite, la description de *l'impact direct* d'une tactique hacktiviste fait référence à l'action directe de Jordan et Taylor. Ce critère permet d'analyser la manière dont sont exposés les impacts immédiats, et non les risques ou le caractère illégal, d'une mobilisation hacktiviste.

Finalement, comme relevé par Jordan, la *notion de la masse d'individus* participant à une mobilisation — en contradiction à une masse d'information — est une notion essentielle visant à légitimer ou non une action collective prenant place dans le cyberespace. Dans cette mesure, il est pertinent de voir comment cette légitimité acquise par la participation de masse est abordée dans les discours.

CHAPITRE 4 : PRÉSENTATION DES RÉSULTATS

4.1 L'identité d'Anonymous

Cette première partie traitera de la manière dont est présenté le collectif dans son ensemble pour ensuite se pencher spécifiquement sur le cadrage des individus prenant part aux diverses mobilisations. L'objectif est d'identifier les stratégies discursives mises de l'avant par les différents acteurs afin de représenter et surtout d'identifier le rapport à l'Autre (Mouffe, 2005). Dans l'étude du cadrage de l'identité d'Anonymous, nous porterons une attention particulière à la manière dont l'esthétisme, le mode d'organisation et les valeurs du collectif sont mobilisés pour décrire des pratiques potentiellement transgressives et, conséquemment, pour identifier une extériorité à l'environnement stratégique néolibéral. Dans l'organisation du collectif, la notion d'anonymat joue un rôle central. Les prochaines lignes viseront à voir comment les enjeux associés à l'anonymat servent au cadrage et à l'identification de l'Autre.

4.1.1 « We are over 9000 » : L'anonymat comme valeur esthétique et organisationnelle

4.1.1.1 Le masque de Guy Fawkes

La notion de l'anonymat est centrale pour identifier le collectif dans les deux types de discours. Cette notion est avant tout véhiculée à travers l'image, l'esthétisme associé à Anonymous. La manière dont les médias véhiculent l'image du collectif est tout à fait cohérente avec l'image et l'esthétisme projetés par ce dernier : les deux discours utilisant plusieurs références identiques (images et portions de vidéo) mettant en

scène les symboles de l'homme en complet sans tête et le désormais fameux masque de Guy Fawkes.

Figure 4.1 Masque et homme sans tête (ABC10, 2010)

Ce dernier est un personnage historique connu pour avoir orchestré la fameuse « Conspiration des poudres » dirigée contre le roi Jacques 1e d'Angleterre en 1605. L'échec de cette conspiration a mené à une fête populaire dans plusieurs pays du Commonwealth, le « Bonfire Night » ou le « Guy Fawkes Night », commémorant et fêtant, tous les 5 novembre, l'arrestation du personnage. L'image du conspirateur est également reprise dans la bande dessinée « V for Vendetta » (Moore & Loyd, 1982) et dans son adaptation cinématographique (McTeigue, 2006). Dans ces œuvres, le personnage de « V » crée son masque à l'image de Guy Fawkes qu'il perçoit comme un défenseur des libertés. De cette manière, Guy Fawkes ainsi que le masque à son image sont utilisés par le collectif, revêtant d'un symbolisme transgressif. Effectivement, le personnage, tout comme l'esthétique qu'il supporte, est représenté comme un conspirateur agissant au nom de ce qu'il perçoit comme l'intérêt général.

Bien que cette image soit utilisée par les deux discours, il semble important de noter que dans le discours des militants, les deux symboles sont représentés dans des proportions équivalentes. Les documents médiatiques à l'étude utilisent beaucoup

plus souvent le masque de Guy Fawkes pour représenter le collectif, au détriment de l'homme en complet sans visage. De manière encore plus importante, l'identification du collectif à l'aide de ces symboles est faite uniquement dans une mince proportion des articles présents dans le corpus des documents médiatiques (six articles sur un total de trente-quatre). Cinq de ces six articles sont des reportages vidéo.

4.1.1.2 Anonymat et organisation dans le discours des médias

Si le masque est associé à une forte symbolique sociopolitique et culturelle, il n'en reste pas moins que, dans la majorité des discours médiatiques, il fait référence à l'anonymat reflété par l'opacité et l'incompréhension de la structure interne du collectif. Cette opacité est liée à l'incapacité de connaître le nombre de militants participant aux opérations, leur identité lors de manifestations hors-ligne et leurs modes de communication tactique. L'anonymat est donc associé à la transgression dans le discours des médias dans la mesure où il rend le collectif presque imprévisible. Effectivement, les médias réfèrent surtout à Anonymous comme une « secretive organization » (MSNBC News, 2011), un réseau décentralisé (Olderman, 2010 ; Pham, 2010 ; Dwyer, 2010) ou un « loose band of so-called hacktivists » (Bouldon, 2010). Les réseaux sur lesquels sont coordonnées les mobilisations, les IRC, sont, quant à eux, décrits comme des réseaux de communication secrets et sécurisés. Ils sont ainsi associés à un manque de transparence: « They communicate in secret internet chat rooms. In public protests, they hide their identity behind masks » (Gordon, 2011b). Cette structure opaque et décentralisée semble également amener une confusion autour du nombre de personnes prenant part aux activités du collectif. Alors que certains articles estiment à quelques milliers le nombre de participants – le nombre de militants connectés sur les IRC durant l'*Operation : Payback* s'élevant jusqu'à 3000 (Shuetter, 2011) — d'autres les estiment à plusieurs dizaines de milliers – en se basant sur les 27 000 et 43 000 téléchargements du LOIC

(Dwyer, 2010). Ce nombre pourrait s'élever jusqu'à plusieurs centaines de milliers de militants (Fox News, 2010d).

Cette incapacité d'identifier et de connaître le nombre de personnes prenant part aux mobilisations d'Anonymous rend le collectif imprévisible. Cette imprévisibilité est très souvent associée à des enjeux sécuritaires. À ce titre, Lisa Stark, journaliste pour ABC News, soutient qu'« Anonymous is a loose network of Internet hacker from around the world. That makes it so much more difficult to know what they're going to do next [...], much more difficult to stop them » (Stark et Muir, 2012). Le même enjeu sécuritaire est relevé par Adam Shapiro du réseau Fox News :

> And it's not the same as when you have the Chinese going after the US intelligence computer, the Russians shutting down Estonian computers to get ready to invade Georgia. This is literally thousands, perhaps hundred of thousands, at one point, people who are, for lack of a better term, angry [...].How do you go after hundred of thousands of people? (Fox News, 2010d).

Bien que le discours des médias ne soit pas exhaustif quant au cadrage du collectif dans son ensemble, il n'en reste pas moins que la notion de l'anonymat rend la tâche d'identifier la structure du collectif à partir de repères connus (structure de pouvoir au sein des États ou dans l'armée, par exemple) particulièrement difficile. Cela mène nécessairement à la construction d'une image menaçante du collectif pour l'ordre social, politique et économique en place.

4.1.1.3 Anonymat et organisation dans le discours des militants

Tout comme dans le discours des médias, la notion de l'anonymat dans le discours des hacktivistes sert à cadrer la structure organisationnelle du collectif comme éminemment transgressive. Cependant, si, dans le discours précédent, cette transgression était liée à des enjeux sécuritaires, elle est ici majoritairement rattachée

à des enjeux éthiques. Effectivement, la notion de l'anonymat est implicitement mobilisée dans les discours militants et est directement liée à la formation d'une identité inclusive, basée sur l'ouverture populaire du collectif. L'image 4.2 présentant une série de personnes éparpillées se ralliant pour former l'homme en complet sans tête, symbole d'Anonymous, illustre efficacement cet objectif. Il est également pertinent de noter l'importance accordée à la définition du collectif (plutôt que les individus faisant partie de ce dernier) dans le discours des militants.

4.2 Anonymous (Anonyme, 2010e)

Alors que l'identité pourrait être construite en tension avec les cultures web dont Anonymous est issu, elle semble plutôt prôner l'utilisation de symboles collectifs. Effectivement, de nombreuses allusions à la constitution américaine sont faites, notamment par la répétition fréquente de ses premiers mots « we, the people » (Anonyme, 2010c; Operation Payback, 2010), de l'expression « the people » (Operation Payback, 2010; Anonyme, 2010c, Anon2) et de la locution « we are the people » (A message from Anonymous, 2010; Operation Payback, 2010; Anonyme, 2010c). Anonymous soutient ainsi que ses rangs sont composés par « the people

representative of many parts of the world and all political orientation » (A message from Anonymous, 2010) et que sa structure est gérée non pas par des leaders définis, mais par des idées : « Anonymous has a decentralized command structure that operates on ideas rather than on directors » (TheHairyHart, 2010). Ainsi, sa structure est changeante et dépend des *Anons* qui la composent, tel qu'il est noté dans un des communiqués de presse : « Anonymous is not always the same group of people : Anonymous is a living idea. Anonymous is an ideal that can be edited, updated, remanded – changed on a whim » (A message from Anonymous, 2010). Les critères d'inclusion relèvent donc de l'adhésion aux valeurs portées par les mobilisations spontanées du collectif – « Any individual, organization, corporation, and/or government entity which supports Freedom of Speech and free Internet is an ally of Anonymous » (A message from Anonymous, 2010).

Ce désir de servir le *bien commun* et le *peuple* est également véhiculé dans l'argumentaire faisant appel au bon sens de la population et usant des valeurs éthiques mises de l'avant par le collectif, créant de ce fait une distance conceptuelle entre ce qui est légal, illégal et juste : « The man on the street already knows this. He knows it when he illegally gives his unused software to a friend or acquaintance. He knows when he gives that old college book to a person in need. However, he also knows that something is wrong » (Operation Payback, 2010). L'identité entourant le caractère populaire et inclusif d'Anonymous se fait ainsi conjointement avec l'identification d'un ennemi, permettant de cette manière à Anonymous de se positionner en tant que « justicier du cyberespace » en affirmant que le collectif est « on your side, standing up for your rights » (Anonymous6499, 2011). Les enjeux éthiques, quant à eux, sont surtout présentés comme des situations politiques, économiques et légales présentées comme injustes : « You have ignored the people, attacked the people, and lied to the people. For this, you will be held accountable before the people, and you will be punished by them » (Operation Payback, 2010).

L'Autre est souvent représenté par des gouvernements, organisations ou corporations décrits comme corrompus (Anonymous Anarchy, 2010; Operation Payback, 2010; Anonyme, 2010a). Cette opposition claire entre le « eux » et le « nous » est premièrement établie à travers un argumentaire qui cadre certaines pratiques de gouvernance comme immorales et qui incite les citoyens à se rebeller: « When governments and corporations control information they control you. When governments are allowed the power of censorship, they are able to commit great atrocities and act in corrupt ways – free from scrutiny of those from who their power derives » (A message from Anonymous, 2010). Elle est deuxièmement introduite par l'interpellation directe des ennemis du collectif : « Corrupt governments of the world. We are Anonymous » (Anonymous Anarchy, 2010). La corruption est associée à des pratiques de gouvernance ne servant pas l'intérêt du public :

> [The man on the street] know that it is not right when his leaders inexplicably support massive capitalist enterprises over the majority opinion of their own people. He know they are wrong when they use illegal means to get what they want, while hypocritically deprecating their opponents for doing the same (Operation Payback, 2010).

L'esthétisme et les pratiques du collectif sont grandement liés à la sous-culture web du trolling sur la plateforme 4chan. Alors que plusieurs références directes à cette culture sont faites à travers la configuration technique du LOIC[33], celles-ci sont très peu nombreuses dans le corpus. La première allusion notée relève de l'identification

[33] Le message apparaissant envoyé sur les sites lors de l'erreur de service inscrit « Ya dun goofed ». Cette énonciation a été faite par le père de Jessi Slauter. Alors que celle-ci se faisait *troller* suite à ses vidéos controversées, le père a explosé de rage devant la caméra web en disant qu'il allait contacter la cyberpolice – ravivant de ce fait le plaisir des *trolls*. La phrase « Ya dun goofed » (pouvant être traduite par « vous avez fini de *niaiser*») est le message envoyé aux sites ciblés par les actions. « IMMA CHARGIN MAH LAZOR » est une référence à un personnage du dessin animé «Dragon Ball Z » , « Shoop Da Whoop » qui crache de manière aléatoire des rayons laser. Cette référence est inscrite sur l'icône permettant le bombardement de données envers un site. L'icône « Fuckin' HIVE MIND » permet au militant de joindre un botnet de manière volontaire. Elle fait référence à la série de science fiction « Star Trek » et aux « borgs », créatures cybernétiques rassemblés à travers une conscience groupale.

primaire du « nous » à travers un élargissement des personnes touchées par le message et les enjeux qu'il supporte. Effectivement, le fait d'entamer un communiqué par « to our fellow *Anons*, /b/retheren, and to the internet as a whole » (Anonyme, 2010b) démontre clairement la volonté du collectif à vouloir inclure non seulement les individus déjà impliqués dans le collectif et les « geeks » déjà actifs sur la plateforme/b/de 4chan, mais l'ensemble des usagers de l'Internet.

4.3 LOIC (Know Your Meme, 2014b)

Finalement, Anonymous fait référence au nombre d'individus prenant part aux activités du collectif en disant « We are over NINE THOUSAND » (Anonymous Anarchy, 2010). Cette énonciation, s'avère être une manière de se moquer de la tendance de l'adversaire à vouloir connaître le nombre d'individus impliqués dans le collectif. Effectivement, vu l'anonymat des participants, il est presque impossible de cerner, même au sein du collectif, le nombre de personnes prenant part aux mobilisations. Ainsi, l'énoncé fait référence à l'accroche du dessin animé japonais « Dragon Ball Z » utilisée sur 4chan dans la création d'un grand nombre « memes [34] ».

[34] Voir glossaire

4.4 **« It's over 9000! » (Know Your Meme, 2014)**

La locution représente « an innumerable quantifier to describe a large number of something like ''several'', ''lots'', ''butt loads'' and even the metric ''ass tonne'' » (KnowYourMeme, 2014). De cette manière, cette énonciation est à la fois une référence directe à la sous-culture de 4chan, une réitération de l'anonymat des participants et de son impact sur la structure organisationnelle du collectif, ainsi qu'une manière de fournir à l'adversaire une information « codée ». Cette information amènera potentiellement l'adversaire à faussement interpréter le mode de fonctionnement du collectif. Cela renforcera, par la même occasion, son opacité de son organisation et accentuera son caractère transgressif.

En somme, l'esthétisme du masque doublé de la notion de l'anonymat permet au collectif d'atteindre une notoriété symbolique extérieure aux groupes de militants. Celle-ci se veut porteuse du caractère inclusif primordial au collectif : celui que tout le monde peut devenir Anonymous. Le discours d'Anonymous accorde une très grande importance à la définition de l'identité du collectif. Tel qu'abordé dans les

paragraphes précédents, celle-ci passe par l'identification de l'adversaire, par la mise en valeur d'une structure organisationnelle perméable et inclusive et par l'effacement de l'individu derrière la collectivité, tant dans l'identification esthétique que dans l'exercice du leadership. Toutes ces manières d'aborder l'anonymat visent à poser Anonymous en tant que force transgressive et agissant à titre de justicier du cyberespace.

4.1.2 L'éthique du hacker

Les informations relatives aux valeurs supportées par Anonymous se rattachent dans les deux corpus à ce que Levy qualifie d'éthique du hacker (Levy, 1985). Ainsi, il sera question de voir comment sont mobilisées les notions de la liberté d'expression et de l'information, de la méfiance envers l'autorité ainsi que de l'opposition au principe du « copyright » dans le discours des médias et dans celui des militants.

La liberté d'expression, la liberté d'information ainsi que l'opposition aux valeurs supportées par la législation entourant le « copyright » sont présentées de manière cohérente dans les deux corpus de discours. Effectivement, dans le corpus de documents médiatiques, plus des trois quarts des énoncés associés aux valeurs supportées par Anonymous sont soit des citations *d'Anons* interviewés, soit des extraits des communiqués de presse diffusés par le collectif. Anonymous est décrit comme le « "first line of defense" against attacks on online freedom » (Sciutto et al., 2010). On dit qu'il combat la censure et le « copywrong » (Olderman, 2010), que ses mobilisations « [revolve] around the idea that information is free » (Housh, 2011) et qu'il vise à obtenir « unlimited freedom of expression » (CNN Writer Staff, 2010). Cependant, ces citations servent souvent à un argumentaire mettant de l'avant des enjeux légaux ou sécuritaires qui délégitimisent les mobilisations : « the philosophy of Anonymous is to make all information free for everyone, regardless of copyright

laws or national security considerations » (Fox News Associated Press, 2011). Un autre article confronte les valeurs mises de l'avant par le collectif avec l'impact de leurs actions : « Wikileaks supporters claim to be "in favor of free speech yet, they attack Sarah Palin for exercising her free speech » (Pham, 2010).

Le discours mis de l'avant par les *Anons* est, quant à lui, avant tout teinté d'un grand enthousiasme technologique où la liberté de l'information est directement reliée à la capacité de créer un monde meilleur:

> The Internet is one of the last bastions of the free flow of information in our revolving information society, and the one that is capable of connecting us all. Through the Internet, all the people of the world have access to information. When we all have access to information, we are strong. When we are strong, we possess the power to do the impossible – to make a difference, to better our world. (A message from Anonymous, 2010)

De cette manière, l'accès aux technologies numériques ainsi que la neutralité du web sont cadrés comme des droits humains : « in these modern times access to the Internet is fast becoming a basic human right. Just like any other basic human right, we believe that it is wrong to infringe upon it » (Anonymous Anarchy, 2010). Selon cette perspective, les valeurs inhérentes à l'éthique du hacker sont associées à des enjeux éthiques. Effectivement, alors que la première phase de l'*Operation : Payback* visait principalement à restreindre des acteurs militants pour le renforcement des lois sur la propriété intellectuelle, le discours d'Anonymous cadrait les pratiques illégales de partage de fichiers comme une atteinte à la liberté personnelle : « As in the past times with the invention of the printing press, it is today that the people embrace this revolution, this new anarchy of freedom to share, while their authocratic rulers seek to crush this freedom » (Operation Payback, 2010).

De cette manière, si la liberté de l'information est liée à la capacité des citoyens à faire des choix politiques plus éclairés et que le piratage informatique de fichiers protégés « democratizes knowledge and makes education affordable » (Operation Payback, 2010), il n'en reste pas moins que les stratégies argumentatives d'Anonymous visent également à déconstruire les arguments de l'adversaire avant de mettre en évidence que les pratiques entourant la gouvernance du web ne sert pas l'intérêt général, mais vise plutôt à l'enrichissement d'une minorité :

> [these] organizations carefully omit the fact that only a small percentage of the profits made by big media ever make it to those who actually produce it. Do they ever disclose how small of a percentage most script writers, novelists, etc., actually make ? Of course not, and there is a reason why. Do these anti-piraxy organizations truthfully disclose how much they receive in donations and from whom ? Of course not, and there is a reason for this also (Operation Payback, 2010).

L'énonciation de ces enjeux d'ordre éthique s'établit de concert avec la définition d'un Autre corrompu, marquant la méfiance qu'entretiennent les militants avec les figures d'autorité (Levy, 1985) ainsi que la position antagoniste dans laquelle ils se posent : « Indeed, the sequestration of human knowledge for the benefit of extremist capitalism is trason against the whole humanity » (Operation Payback, 2010).

4.1.2.1 Conclusion partielle

La section précédente a permis de relever deux jalons principaux. Le premier est la divergence des enjeux rattachés à la description de la structure interne et des valeurs mises de l'avant par le collectif dans les deux corpus à l'étude. Effectivement, les enjeux sécuritaires et légaux rapportés dans les discours des médias placent le collectif comme une menace potentielle à l'ordre en place et cadrent sa structure organisationnelle basée sur l'anonymat comme transgressif. Cette adversité est également présente dans le discours des *Anons* qui opposent drastiquement leurs

valeurs à celles supportées par le système actuel. En identifiant clairement un ennemi, le collectif promeut une structure organisationnelle où l'individu s'efface au profit de l'ensemble, permettant la construction d'une identité collective de justicier du cyberespace, basée sur le principe que tout le monde peut potentiellement devenir Anonymous.

Les deux discours positionnent ainsi délibérément Anonymous comme un acteur transgressif, tant au niveau organisationnel que des valeurs qu'il supporte. À cet effet, un gazouillis de John Perry Barlow, membre fondateur de la Electronic Frontier Foundation, est utilisé à plusieurs reprises dans les deux corpus de documents et démontre bien la dynamique de confrontation entre les valeurs supportées à travers les deux discours : « The first infowar is now engaged. The field of battle is Wikileaks. You are the troops » (Barlow, 2010).

4.1.3 Qui sont les hacktivistes ?

Après avoir abordé la manière dont était cadré le collectif dans son ensemble, il sera ici question de cerner la manière dont sont décrits les individus prenant part aux mobilisations de l'*Operation : Payback.*

4.1.3.1 L'effacement de l'individu au profit de la collectivité

Les extraits codés à cette thématique dans le corpus de documents publiés par Anonymous sont très peu nombreux. De manière cohérente avec leur définition du collectif, les *Anons* soutiennent que ce dernier est composé « with the people representative of many parts of the world and all political orientations » (A message from Anonymous, 2010) et que ses différentes opérations mobilisent différents

groupes d'individus. De cette manière, la diversité des opinions au sein du collectif est définie comme une des caractéristiques principales de son identité : « Anonymous » past is not our present. May we remind you that Anonymous is a dynamic entity. Furthermore, anything attributed, credited, or tagged to Anonymous is not always based on the consensus of us as a whole » (A message from Anonymous, 2010). En soutenant qu'il est composé « of people with diverse points of view, of which not all coincide with one another. » (Anonymous6499, 2011), le collectif établit un lien clair entre son identité et celle des individus qui le composent. D'une part, son discours prône l'anonymat des participants et l'effacement de l'individu derrière le groupe et, d'une autre part, il attribue une grande importance aux individus dans le choix et dans les orientations de ses mobilisations à travers un mode de gouvernance pouvant se rapprocher de la démocratique directe. Finalement, le collectif ne se définit pas comme un groupe de *hackers*, mais plutôt comme un groupe d'usagers de l'Internet, sans connaissances techniques particulières : « Anonymous is not a group of hackers. We are average Internet citizens ourselves » (TheHairyHart, 2010), renforçant ainsi l'idée selon laquelle tout le monde peut potentiellement devenir Anonymous.

4.1.3.2 Militant, vandale ou virtuose technique ?

Le discours des médias se montre beaucoup plus diffus et confus relativement à la qualification des individus prenant part aux mobilisations du collectif. En effet, ceux-ci sont définis à la fois selon les activités qu'ils mènent sur l'Internet, selon les valeurs que celles-ci supportent ainsi que selon leurs connaissances techniques. Les prochains paragraphes exposeront premièrement la manière dont sont définis les hacktivistes en abordant ces deux thématiques. Puis, il sera question de voir en quoi ces définitions permettent de noter un écart entre la compréhension des activités de militance et la construction sémantique d'une menace véhiculée par les hacktivistes.

La caractérisation des militants en fonction des activités qu'ils mènent sur l'Internet s'oriente autour de deux axes : celui de l'activisme politique et celui des valeurs politiques défendues à travers cet activisme. D'entrée de jeu, le champ lexical de la militance n'est que très rarement exploité pour décrire les *Anons*. Effectivement, les qualificatifs « online activists », « web activists », « Internet activists » (Rasch et Todd, 2010 ; Schubert, 2010 ; Fox News, 2010c ; Olderman, 2010 ; MSNBC News, 2011 ; Frantz et Schubert, 2010 ; Pham, 2010 ; FoxNews, 2010a) ainsi que le terme « hacktivist » et ses dérivés ne sont qu'employés à vingt reprises parmi les 180 extraits codés dans la thématique « description des hacktivistes ». De plus, plusieurs d'entre eux sont précédés ou suivis de courtes expressions remettant en question la crédibilité du terme utilisé, comme dans les locutions « they call themselves hacktivists » (Fox News, 2010d), « they call themselves activists » (MSNBC News, 2011) et « so-called hacktivists » (Bouldon, 2010 ; Hunt et MacFarland, 2010 ; Gordon, 2011b ; Sciutto, 2010). Dans de rares occasions, si l'extrait rapporte efficacement la notion de militance et de mobilisations populaires, il reste pourtant néanmoins associé, dans l'argumentaire mis de l'avant dans le paragraphe ou dans les propos généraux de l'article, à une connotation négative qui associe les pratiques de militance à des enjeux, pour la plupart, d'ordre sécuritaire. C'est le cas de cet extrait apparaissant dans l'article « The Top Four Cyber Threats for 2011 », publié en ligne par ABC News : « The loosely organized "hacktivists" managed to take down the web pages of several of their targets, and their spontaneous attempt may be the first major showing of a new way to express political beliefs at a grassroots level » (ABC News, 2011). Dans cet article, le hacktivisme – et la notion de militance qui s'y rattache — est présenté comme la deuxième menace de l'année, aux côtés de la

cyberguerre et du virus Stuxnet[35], du SPAM et des fraudes monétaires sur les réseaux mobiles.

Le second axe relève de l'association entre les militants et les valeurs prônées par Wikileaks. Effectivement, un peu plus de 30 extraits codés sous la thématique « description des hacktivistes » associent directement les *Anons* à Wikileaks. Les militants sont décrits comme des « Wikileaks supporters », « allies on the Internet », « Assange's supporters », etc. (Sciutto, 2010 ; Pham, 2010 ; Sciutto et coll., 2010 ; Dwyer, 2010 ; ABC News, 2011 ; Bouldon, 2010 ; Smith, 2010 ; CNN Writer Staff, 2010 ; Gross, 2011 ; Shuetter, 2011 ; FoxNews, 2010a ; Fox News Associated Press, 2010 ; Fox News, 2010b ; Fox News, 2010c ; Fox News, 2010d ; Hunt et MacFarland, 2010 ; Fox News, 2010e ; Olderman, 2010). Nous avons donc analysé la manière dont était abordé Wikileaks afin de pouvoir rattacher une connotation et associer des enjeux à l'identification des militants décrits comme des sympatisant de Wikileaks.

Les enjeux les plus souvent abordés relatifs à la description de Wikileaks et de son porte-parole Julian Assange sont d'ordre sécuritaire, légal et éthique. En premier lieu, la totalité des enjeux éthiques est abordée en lien avec des enjeux sécuritaires par l'entremise de citations de l'ancienne gouverneure de l'Alaska et candidate à la vice-présidence des Etats-Unis, Sarah Palin. Effectivement, celle-ci a publiquement accusé Assange d'être « an anti-american operative with blood on his hands » (Shuetter, 2011 ; Pham, 2010 ; Fox News Associated Press, 2010), elle a qualifié Wikileaks de « shady disreputable organization with no regard for laws or human life » (Pham,

[35] Voir glossaire

2010) et ses activités, d'être de « sick, un-American espionnage efforts » (Sciutto, 2010 ; Pham, 2010 ; Sciutto et al., 2010 ; Fox News Associated Press, 2010). Les enjeux sécuritaires, quant à eux, mettent davantage l'accent sur la publication de plus de « 250 000 secret U.S. diplomatic cables » (ABC News, 2011 ; Ryan, 2011a ; Fox News, 2010b ; Fox News, 2010e). L'enjeu juridique reste cependant le plus fréquemment utilisé — annonçant l'arrestation du porte-parole, recherché en Suède pour des crimes sexuels (Sciutto, 2010 ; ABC News, 2011 ; Bouldon, 2010 ; CNN Writer Staff, 2010 ; Frieden et Candiotti, 2011 ; Fox News, 2010b ; Fox News, 2010c ; Fox News, 2010e).

Ainsi, le fait de présenter les militants comme étant des *Wikileaks supporters* permet aux discours des médias de rattacher leur identité à la fois à des enjeux éthiques liés aux prises de position publiques de Palin à l'égard de Wikileaks, à des enjeux sécuritaires entourant les fuites de documents et, surtout, à des enjeux juridiques et moraux émanant des accusations de viol portées contre Julian Assange.

La seconde thématique entourant la caractérisation des militants relève des connaissances techniques de ceux-ci. Un nombre limité d'articles identifient le militant comme ayant des connaissances techniques restreintes. Bien qu'il soit mentionné à quelques reprises qu'il est « relatively simple for supporters to install [LOIC] on their computers » (Fox News, 2010e) et qu'il n'est plus nécessaire, à l'heure actuelle, d'être un virtuose technique pour mener ce genre d'attaques (Housh, 2011), ce n'est pas les propos qu'avancent la majorité des articles. Effectivement, l'utilisation fréquente du mot « hacker » et « pirate » pour décrire les *Anons* – utilisé plus de 75 fois dans le corpus – doublés du visuel mobilisé – i. e *le hacker* solitaire, les derrières d'ordinateurs avec une multitude de fils entremêlés ainsi que des mains tapant sur un clavier faisant défiler une série de codes binaires – créent un imaginaire

autour de la figure du hacktiviste qui se rapporte davantage à un virtuose technique. Pourtant, les outils techniques mobilisés dans les campagnes d'Anonymous, tel que le LOIC, ne relèvent pas d'une grande complexité et peuvent aisément être utilisés par des *script kiddies*. Cela amène une discordance entre les images utilisées pour décrire les acteurs derrière les mobilisations d'Anonymous et la réalité technique de celles-ci.

Ainsi, le caractère décentralisé du collectif et l'image du *hacker* véhiculé dans plusieurs discours médiatiques tendent à le représenter comme dangereux non pas par la portée de ses actions immédiates, mais à travers la menace qu'il représente. Effectivement, deux militants qualifiés de *hackers* sont incarnés dans le discours des médias. Le premier est interviewé uniquement dans un article. Il est présenté comme un « 29 years old, cocky college drop out » (MSNBC News, 2011) et est perçu à l'écran comme anarchiste fumeur, toujours filmé près de son ordinateur et de son bureau désordonné et truffé de vieilles cigarettes. Le second « hacker » en est un de seize ans, arrêté aux Pays-Bas suite à l'*Operation : Payback* (Dwyer, 2010 ; CNN Writer Staff, 2010 ; Frieden et Candiotti, 2011 ; Fox News, 2010b ; Kaplan, 2010 ; Hunt et MacFarland, 2010 ; MSNBC News, 2011). Alors que l'un incarne un marginal rebelle, le second, beaucoup plus abordé dans le corpus, est présenté comme la figure du jeune « geek », du *hacker* hollywoodien ; les deux étant liés dans la mesure où ils incarnent des individus asociaux, solitaires et marginaux. Cette image est utilisée, notamment dans le reportage « Anonymous' Hackers High Profile Targets » diffusé sur le réseau ABC, pour dresser le portrait d'une menace :

> The arrest of this 16 years old boy accused of being a hacker is a sign of a bigger threat. [...] Put an army of young people like that together and you have a glimpse of the wars to come. This yound man, a computer expert [...] using a server in the nearby dutch town of Haarlem to cause chaos right across the Internet (Hunt et MacFarland, 2010).

4.1.4 De la collectivité à l'individu

Afin de conclure cette section portant sur l'identité d'Anonymous, il serait pertinent de noter l'attention portée par chacun des discours à l'étude aux deux thématiques proposées : celle de l'identité du collectif et celle de l'identité des individus formant le collectif. Alors que dans le corpus de documents produits par Anonymous, une majorité d'extraits visent à définir le collectif dans son ensemble plutôt que les individus prenant part aux mobilisations, les médias tentent davantage de définir les individus plutôt que la structure identitaire du collectif dans son ensemble. D'une part, cette constatation simple peut aisément être rattachée au besoin du collectif à légitimer sa structure, ses valeurs et ses actions – celles-ci étant perçues comme des vecteurs de mobilisation de masse. D'autre part, la stratégie des médias visant à identifier les individus afin de décrire le collectif pourrait viser, quant à elle, à désintégrer l'action de masse des militants. Cela permettrait de les conceptualiser non pas comme un groupe véhiculant un message politique, mais comme des virtuoses « fâchés » (Sciutto et coll., 2010 ; Dwyer, 2010 ; Fox News, 2010d), imprévisibles et, conséquemment, menaçants pour le système en place.

4.2 Cadrer l'*Operation : Payback*

Les prochaines pages viseront à répondre directement à la seconde sous-question de recherche portant sur le cadrage de l'Operation : Payback et, par la même occasion, à la quatrième sous-question portant sur les enjeux mis de l'avant par un discours afin de supporter un cadrage spécifique. Celles-ci seront abordées en deux temps. Dans un premier temps, il sera question d'examiner les objectifs et le déroulement de l'opération en général selon les cadrages effectués à travers le discours des *Anons* et dans celui des médias. Ainsi, nous nous pencherons spécifiquement sur la manière dont sont présentées les « cibles », les motivations entourant les actions des militants

ainsi que les objectifs des mobilisations. Dans un deuxième temps, nous traiterons du cadrage des différentes tactiques mobilisées dans l'Operation : Payback. En tenant pour acquis que ces pratiques de militance sont relativement nouvelles, une attention particulière sera donc portée à la manière dont la nature technique des tactiques, la légalité de celles-ci ainsi que leur impact immédiat sur l'adversaire sont décrits dans les deux types de discours. Nous verrons ensuite comment les notions de masse et de non-violence, inhérentes au NVDA et à son homologue virtuel, le MVDA (Jordan, 2002), sont utilisées pour légitimer ou délégitimer les tactiques hacktivistes.

4.2.1 Qualifier les mobilisations

Il a été énoncé dans la section portant sur la présentation du cas que l'*Operation : Payback* a été menée en deux phases. La première est liée à des mobilisations contre les industries du divertissement et contre certains militants « procopyright ». Elle a été déclenchée alors que certaines compagnies ont effectué des attaques par déni de service vers des sites de partage « peer to peer »[36] (Olson, 2012). La seconde phase visait certaines multinationales ayant retiré leur support financier à Wikileaks pour cause de « non-respect des normes d'utilisation » (Olderman, 2010). Les prochains paragraphes aborderont ces deux phases. Il y sera argumenté que le discours des médias tend à occulter le caractère politique des deux phases des mobilisations, alors que le discours d'Anonymous vise presque exclusivement à définir et à légitimer les enjeux éthiques sous-tendant leurs pratiques et à mettre de l'avant leur caractère politique.

[36] Voir glossaire

4.2.1.1 Identification des adversaires et motivations dans les discours des médias

D'entrée de jeu, il est important de noter que le corpus de documents médiatiques se concentre presque exclusivement sur la seconde phase des mobilisations. Alors que 32 articles se consacrent à couvrir les mobilisations entourant Wikileaks, seulement deux abordent la première phase. Effectivement, un article traite de l'arrestation d'un membre du groupe Anonymous pour avoir « allegedly shut down [...] with a distributed denial of service attack » (Ryan 2011b) la page web personnelle du chanteur Gene Simmons du groupe KISS qui avait récemment participé à une « anti-piracy conference and called for a crackdown on file and music sharing on the Internet » (Ryan 2011b). L'article suivant énumère les principaux organismes gouvernementaux et corporations ciblés par les mobilisations d'Anonymous et soutient que « the attacks were retaliation against the discontinuation of "The Pirate Bay," a Sweden-based file sharing website devoted to the illegal downloading of copyrighted material. » (Fox News Associated Press, 2011) Les « cibles » d'Anonymous sont donc identifiées comme étant soit des individus qui ne partagent pas les idéaux du collectif (Ryan 2011b), soit comme des organisations dont les activités visent à restreindre des pratiques décrites comme illégales. Les articles attirent l'attention du lecteur sur la criminalité de l'action en mettant en premier plan l'arrestation des militants et en présentant les accusations portées à leur égard : « [They were] arrested today after being charged in an indictment with conspiracy and unauthorized impairment of a protected computer » (Ryan 2011b).

Les documents traitant des mobilisations entourant Wikileaks adoptent un discours similaire. Tel qu'il a été abordé précédemment, si les individus prenant part aux mobilisations sont qualifiés de défenseurs de Wikilea*ks*, leurs motivations sont souvent décrites comme étant de la « vengeance » envers les corporations ayant cessé leurs liens commerciaux avec Wikileaks (Sciutto, 2010 ; Dwyer, 2010 ; Ryan 2011b ; Bouldon, 2010 ; Schubert, 2010 ; Smith, 2010 ; Frieden et Candiotti, 2011 ; Fox

News, 2010[e] ; Olderman, 2010 ; MSNBC News, 2011 ; Gordon, 2011a ; Gordon, 2011b). Ainsi, bien que les mobilisations soient présentées comme des actions spontanées, quelques articles vont plus loin en les associant à des motifs d'ordre émotionnels découlant de la rage et de la colère : « [their] interest is [...] keeping Wikileaks online and taking out their anger, [...] [on] those organizations they deem responsible for keeping Wikileaks in trouble » (Fox News, 2010d). De cette manière, les actions militantes tendent à être conceptuellement dissociées de leurs principes politiques et éthiques, ceux-ci n'étant pas présentés comme réfléchis et rationnels. Cela peut être associé à l'image du jeune *hacker* présenté comme un individu présocialisé et dont les émotions non muries peuvent donner lieu à des excès de rage.

Bien que la majorité des extraits codés se rattachent à ce point, trois autres motivations sont également relevées. En effet, la politicienne Sarah Palin a été ciblée dans *l'Operation : Payback* à la suite de l'expression de propos virulents en public. Ainsi, quelques articles notent que le collectif « even hacked into the accounts of politicians who have criticized them » (Sciutto, 2010). Dans ces articles, la divergence d'opinions personnelles est perçue comme la source de motivation des militants. Ensuite, nous notons que lors de l'énonciation des valeurs politiques et des enjeux éthiques motivant les mobilisations et justifiant le choix des cibles, ceux-ci sont directement décrits comme défendant des pratiques illégales : « Operation : Payback has attacked organizations they thought to be involved in Internet censorship and media companies trying to shut down illegal file-sharing sites » (Fox News, 2010d). Dans cette optique, la notion de légalité est mobilisée afin de délégitimer le discours adversaire. Finalement, deux extraits lient les motivations des hacktivistes à celles des *hackers.* Kevin Mitnick, soutient à cet effet que les hacktivistes « want to prove to the FBI that they're smarter. And they want to embarrass the FBI » (Stark et Muir, 2012). Dans le même ordre d'idée, le « former federal prosecutor Matthew Yarbrough » (Gordon, 2011a) réfute complètement la possibilité d'un activisme politique derrière ce type d'attaques en disant que « [m]ost people who are doing this

are doing it for power - or [what] they claim to be activism, [...] but they're really doing it so they can brag about it » (Gordon, 2011a).

4.2.1.2 Identification des adversaires et motivations dans le discours d'Anonymous

L'argumentaire mis de l'avant dans le corpus des documents diffusés par les *Anons* vise, quant à lui, tout d'abord à légitimer les pratiques militantes par le choix des cibles et par la défense de la liberté de l'information au nom de l'intérêt commun. D'emblée, tous les documents d'Anonymous annoncent clairement que leurs pratiques de militance ne visent ni à avoir un impact néfaste sur les utilisateurs des organismes ou compagnies ciblés (Anonymous6499, 2011) ni à atteindre des infrastructures critiques :

> We do not want to steal your personal information or credit card numbers, we also do not seek to attack critical infrastructure of companies such as MasterCard, Visa, PayPal or Amazon. Our current goal is to raise awarness about Wikileaks and the underhand methods employed by the above companies to impair the ability of Wikileaks to function. (TheHairyHart, 2010)

Les cibles sont donc choisies de manière réactive à un événement où certains acteurs agissent, selon le collectif, de manière injuste : « they have declared themselves our enemies by sending out thousands of blackmailing letters against innocents, seeking compensation for copyright infringements that don't exist » (Anonymous6499, 2011). Même si ces affirmations peuvent paraitre cohérentes avec celles avancées dans le corpus précédent, il semble néanmoins qu'Anonymous s'attaque plutôt à l'illégitimité des processus entourant la criminalisation du partage de fichiers protégés et la censure d'organismes tels que Wikileaks. À ce titre, Anonymous fait entre autres référence aux actions par déni de service menées par des organismes gouvernementaux envers des sites web tels que thepiratebay.org en disant que « [a man knows] they are wrong when they use illegal means to get what they want, while hypocritically deprecating their opponents for doing the same » (Operation Payback, 2010).

Ainsi, ce qui est défini comme juste et injuste se rapporte directement aux valeurs à la base de l'identité du collectif. Il n'en reste pas moins que dans l'*Operation : Payback,* la notion de liberté d'information joue un rôle particulièrement central. Cette notion est mobilisée tant dans le discours sur la propriété intellectuelle que dans celui sur la censure — que ce soit à travers un meilleur exercice de la citoyenneté promu par une information politique plus transparente ou par le partage de fichiers permettant de rendre l'éducation « plus accessible » (Operation Payback, 2010). Bref, la notion de justice est au centre de l'argumentaire du collectif : « Our motivation is a collective sense of being fed up with all the minor and major injustice we witness everyday » (TheHairyHart, 2010).

4.2.1.3 Finalité des mobilisations dans le discours d'Anonymous

L'*Operation : Payback* compte deux finalités principales selon le cadre établi par Costanza-Chock: celle reliée à la mobilisation et celle reliée au culturel (Costanza-Chock, 2003). En premier lieu, les finalités culturelles révèlent leur caractère transgressif par le fait que les requêtes effectuées ne peuvent être résolues dans le contexte politique et économique actuel. Effectivement, le discours d'Anonymous met de l'avant comme finalité culturelle principale « the freedom of information exchange, freedom of expression and free use of the Internet » (A message from Anonymous, 2010) en soutenant que « a private entity should not have control over the freedom of information » (Anonyme, 2010b). Dans cette mesure, Anonymous se place dans une situation d'antagonisme politique en avançant qu'il est du devoir du collectif de se battre contre « the oppressive future which looms ahead. We have a chance to fight in the first inforwar ever fought » (Anonyme, 2010a).

La finalité liée à la mobilisation, quant à elle, est présentée comme une manière de créer un mouvement populaire autour de ces problématiques. Dans cette optique, si

les finalités définitives résident dans un changement culturel entourant, entre autres, la gouvernance du cyberespace, alors la finalité immédiate est une prise de conscience générale. À cet effet, il est mentionné que leur « current goal is to raise awarness about Wikileaks and the underhand methods employed by the [...] companies to impair the ability of Wikileaks to function » (Anonyme, 2010c). De plus, Anonymous encourage les militants à être créatifs pour attirer l'attention du public afin de s'assurer que « everyone (...) is aware of what is happening » (Anonyme, 2010a). Un communiqué de presse établit un parallèle entre le mouvement en cours et les grands mouvements sociaux américains des années 1960 :

> During the Civil Rights Movement in the United States in the 1960s [...] the protestors [...] managed to make drastic changes to police and governments by refusing to be silenced. In the spirit and memory of that movement and many others we will refuse to be silenced. We will protest.

La communication est ici perçue comme un vecteur de changements profonds par l'implantation graduelle de normes actuellement perçues comme opposées à celles promues par le système en place, se rattachant à ce qu'avance Jordan: « the ethics of the future can only come from transgression, from reaching beyond current ways of negotiating social conflict and resolving differences» (Jordan, 2002).

4.2.1.4 Les finalités des mobilisations dans le discours des médias

Le corpus médiatique s'avère peu exhaustif en ce qui a trait à l'énonciation de la finalité des mobilisations de l'*Operation : Payback.* Les trois quarts des extraits codés à cet effet sont des citations de communiqués de presse diffusés par Anonymous ou des extraits d'entrevues avec des *Anons.* De cette manière, les finalités dites culturelles sont exposées à travers les valeurs de la liberté de l'information et d'expression et par la neutralité de l'Internet (Sciutto et coll., 2010; McDermott, 2012; CNN Writer Staff, 2010; Frantz et Schubert, 2010; Fox News, 2010b; Kaplan, 2010; Fox News, 2010[e]; Olderman, 2010), mais ne restent que très

rarement rattachées à des enjeux. Une seule exception figure dans un article publié sur le site web de Fox News où le journaliste affirme que « the philosophy of Anonymous is to make all information free for everyone, regardless of copyright laws or national security considerations » (Fox News Associated Press, 2011). Il associe directement les normes dites éthiques mises de l'avant dans le discours d'Anonymous avec des enjeux d'ordre économique, légal et sécuritaire. L'adoption de ces valeurs est de ce fait présentée comme quelque chose d'irréfléchi et, donc, d'irrationnel.

4.2.1.3 Conclusion partielle

Tel que le propose le nom de l'opération, *Operation : Payback* est présentée dans le discours des médias comme une revanche prise par les hacktivistes envers « individuals they don't agree with » (Ryan 2011b) ou contre des entités qui assurent le respect des lois. Dans ces articles, les enjeux éthiques mis de l'avant dans le discours d'Anonymous sont totalement évacués. Les motivations entourant les mobilisations ainsi que leurs finalités sont conséquemment présentées, au mieux, comme une divergence d'opinions prenant la forme d'une attaque envers la propriété privée et la liberté d'expression d'un individu de renom et, au pire, comme un soutient illégitime à des activités illégales ou immorales.

4.2.2 Les tactiques

La description des tactiques employées dans les mobilisations d'Anonymous diffère grandement d'un corpus à l'autre. Les prochains paragraphes viseront à cerner quelles sont les stratégies discursives utilisées par les deux discours afin de légitimer ou non le caractère politique et militant des répertoires d'action utilisés. Pour ce faire, une grande importance a été accordée aux champs lexicaux reliés à la guerre, à la criminalité ainsi qu'au militantisme dans la description et la légitimation des actions

techniques d'Anonymous. Il sera argumenté que ces champs lexicaux sont exploités dans les deux corpus, mais de manière différente. Effectivement, alors que le collectif se place conceptuellement dans une situation d'affrontement pouvant se rattacher aux grandes révolutions[37] armées, la description de leurs tactiques se rattache au champ lexical de la militance. Le discours des médias, quant à lui, tend plutôt à cadrer les tactiques comme faisant partie d'une cyberguerre où des hors-la-loi « attaquent » une série d'institutions.

4.2.2.1 Pour le « lulz » et le « payback »

Une variété de tactiques sont présentées dans les documents diffusés par Anonymous. L'ensemble de celles-ci vise à véhiculer un message dans l'espace public et à obtenir de l'attention médiatique par le biais de tactiques conventionnelles ou perturbatrices (Costanza-Chock, 2003). Le collectif fait premièrement appel à des tactiques conventionnelles, c'est-à-dire des appels au boycott (Anonyme, 2010a) et de la diffusion d'information dérangeant peu l'ordre public :

> Get vocal! Twitter, MySpace, Facebook and other social networking sites are critical hubs of information distribution. Make sure everyone you know is aware of what is happening. If you're up for it, print out cable which are relevant to you area and distribute them. Post them on bus stop and train stations, street lamps. Be creative and catch people's attention (Anonyme, 2010a).

Cependant, la majorité des pratiques du collectif sont perturbatrices (Costanza-Chock, 2003). En effet, les appels à la mobilisation encouragent les *Anons* à *doxer*[38] les têtes dirigeantes des entreprises ciblées, à envoyer des « pizza and other crap » (Anonyme,

[37] En faisant notamment appel à la première phrase de la constitution américaine liée à la Guerre d'indépendance des États-Unis
[38] Voir glossaire

2010b) à leur adresse personnelle, à leur faire des coups téléphoniques (Anonyme, 2010b) pour mobiliser indûment leurs lignes téléphoniques ou à leur envoyer des faxes d'encre noire afin de gaspiller leur papier et leur encre. Ces tactiques légales, sont issues des pratiques de *trolling* et visent à obtenir un maximum de « lulz and Payback » (Anonyme, 2010b).

La tactique la plus médiatisée est sans aucun doute l'action par déni de service. Bien que les militants nomment la tactique ainsi que le LOIC dans tous documents, le fonctionnement technique reste explicité seulement de manière marginale. Dans ces articles, ils associent la tactique aux sièges (*sits-in)* non violents effectués au cours des années 1960 en Caroline du Nord, en précisant que ces actions « merely take up bandwidth and system resources like the seats at the Woolworth's lunch counter »[39] et qu'elles ne créent aucun « damage to the computer hardware » (A message from Anonymous, 2010). Aucun document à l'étude n'indique clairement la légalité ou l'illégalité des tactiques promues. L'ensemble du corpus compte uniquement deux références indirectes à leur illégalité potentielle. Le premier article note, à titre d'exemple, les actions par déni de services menées par la compagnie Aiplex envers « thepiratebay.org » et supporte que cette compagnie ait usé d'« illegal means to get what they want, while hypocritically deprecating their opponents for doing the same » (Operation Payback, 2010). Les *Anons* reconnaissent ainsi indirectement l'illégalité de leur tactique en mettant néanmoins l'accent sur le fait que d'autres l'utilisent également sans représailles judiciaires. Le deuxième fait référence aux actes de désobéissance civile ayant eu lieu pendant les années 1960. Ils rapprochent conceptuellement les actions par déni de service à des sièges non violents :

---

[39] Fait référence à quatre étudiants noirs qui, en ayant pris place au comptoir du restaurant Woolworth, en Caroline du Nord, se sont fait refuser d'être servis. Les étudiants ont donc mené un des premiers sit-in ayant participé au déclenchement des mouvements sociaux visant à l'égalité raciale dans le sud des Etats-Unis. Le comptoir en question est aujourd'hui considéré comme un patrimoine historique. (Smithsonia Natural Museum of American History, 2014)

> During the Civil Rights Movement in the 1960s, access to many businesses was blocked as a peaceful protest against segregation. Today much business is conducted on the Internet. We are using the LOIC to conduct distributed denial of service attacks against businesses that have aided in the censorship of any person (A message from Anonymous, 2010).

De cette manière, la légitimité de cette tactique se construit en deux temps. Premièrement, elle est associée à des gestes de désobéissance civile hors-ligne ayant marqué symboliquement et culturellement l'histoire américaine contemporaine. Ensuite, elle est rattachée à une protestation symbolique, visant à faire la publicité et à attirer l'attention des médias plutôt que d'atteindre des infrastructures dites critiques et d'incommoder des citoyens:

> We do not want to steal your personal information or credit card numbers, we also do not seek to attack critical infrastructure of companies such as Visa, MasterCard, PayPal or Amazon. [...] Rather than doing that, we focused on the corporate websites, which is to say, their online public face. It is a symbolic action. As bloggers and academics express it, it is a legitimate expression of dissent. [...] Since the attack got so much attention in the media, we feel that it would affect the people in a negative way and make them feel threatened by Anonymous. Simply put, attacking a major online retailer when people are buying presents for their loved ones would be of bad taste (TheHairyHart, 2010).

Le collectif légitime donc ses mobilisations en énonçant clairement que les impacts des répertoires d'action mobilisés dans l'*Operation : Payback* ne visent ni à atteindre les services de paiements, ni à mettre en ligne les numéros des cartes de crédit des clients de MasterCard et de Visa, mais plutôt à avoir un impact symbolique permettant d'attirer l'attention des médias sur une situation jugée inacceptable.

Ainsi, la notion de non-violence qui, selon Jordan (2002), doit être reconceptualisée dans le cyberespace est implicitement mobilisée dans le discours d'Anonymous. Les

militants rattachent directement leurs protestations à des actes de désobéissance civile traditionnelle et assurent que les actions n'ont causé aucun dommage aux ordinateurs et aux systèmes ciblés. De cette manière, pour Anonymous, les actions par déni de service ne relèvent pas d'un glissement de paradigme relié à la légitimité de l'usage de la violence dans des mobilisations à travers, par exemple, des actes de vandalisme dans le cyberespace. Le collectif soutient intrinsèquement que ses pratiques militantes sont non violentes.

Si le collectif défend ardemment le caractère pacifique de ses tactiques, il met néanmoins de l'avant une image violente en ce qui a trait à l'affrontement de ses ennemis : « Our botnets and war machines will crush you under their treads » (Anonyme, 2010b). Ainsi, les ordinateurs sont décrits comme des « war machines »; le partage de l'information, comme le « greatest weapon to weild » (Anonyme, 2010b); les militants, comme des soldats (Anonyme, 2010b); les enjeux politiques, comme un champ de bataille (Anonyme, 2010a) et l'*Operation : Payback,* comme la première « infowar » (Anonyme, 2010a). Bref, le champ lexical de la guerre véhicule une image violente, mais semble davantage servir au collectif comme une manière de se positionner symboliquement en tant qu'adversaire stratégique dans un environnement stratégique néolibéral.

La notion de masse comme vecteur de légitimation reste très peu abordée dans le discours du collectif. Ceci est sans doute dû au fait qu'il est très difficile d'estimer le nombre de militants participant aux opérations d'Anonymous. De cette manière, cette notion est surtout véhiculée à travers les valeurs supportées par le collectif, celles-ci étant cadrées comme défendant l'intérêt global. En effet, en référant au collectif comme étant « the manifestation of the common will » (Anonyme, 2010b) ou « the voice of the people » (Operation Payback, 2010), Anonymous ne légitime pas ses

actions en fonction du nombre de participants, mais en fonction d'une action portée vers l'intérêt général. Le collectif prétend donc agir au nom de ceux qui ont tenté de se faire entendre en vain : « For some time now, voices have been crying out in unison against the new ACTA laws. The gross inadequacies of the new laws are being passed internationlly have been pointed out repeatedly » (Anonymous Anarchy, 2010). Il est possible de constater dans le discours d'Anonymous une certaine fracture entre la description des actions techniques et la légitimation de celles-ci. Alors que le fonctionnement, l'impact direct ainsi que le caractère non violent des actions par déni de service sont efficacement comparés à leur homologue hors-ligne, le collectif évacue totalement la question de la participation de masse dans ses tactiques techniques. Effectivement, en mobilisant la notion de masse autour de l'intérêt du plus grand nombre, le collectif n'arrive pas à différencier la masse d'individus participant à une mobilisation à une masse de données (Jordan et Taylor, 2004) menant au ralentissement ou à l'arrêt d'un site web.

Les tactiques présentées dans le discours d'Anonymous sont nombreuses et appartiennent à des répertoires d'action autant conventionnels que perturbateurs (Costanza-Chock, 2003). Bien qu'une certaine emphase soit apportée sur les actions par déni de service, il n'en reste pas moins que ces actions ne sont que brièvement définies. De cette manière, nous pouvons avancer que la légitimation des tactiques employées par le collectif ne passe pas par la légitimation de ses processus techniques. Celle-ci passe à la fois par la mise en valeur des principes éthiques soulevés par les actions décrites comme symboliques et visant à la publicité plutôt qu'à l'atteinte d'infrastructure critique et par l'association des tactiques et de leurs impacts à des mouvements de désobéissance civile traditionnels.

4.2.2.2 L'action par déni de service : une nouvelle arme dans le cyberespace ?

Si les documents diffusés par le collectif mettaient de l'avant une série de tactiques déployées dans les mobilisations, le corpus de documents médiatiques identifie uniquement l'action par déni de service. Les termes « attaque », « cyberattaque » et « assaut », utilisés pour décrire les actions par déni de service, sont les mots les plus récurrents dans l'ensemble du corpus, comptant près de 300 occurrences. Il est intéressant de noter que la majorité du champ lexical utilisé pour décrire la tactique se rapproche de celui de la guerre. Effectivement, les termes relatifs à la guerre sont utilisés tant pour décrire les actions du collectif et leur relation avec l'adversaire (i.e « cyberwarfare », « war of data », « cyber battles ») que pour définir leurs actions techniques — les actions par déni de services étant décrites comme un « bombardement » de données envers des « cibles » données. Cette analogie est poussée à l'extrême dans un reportage de Fox News où une experte de cybersécurité, en parlant de l'arrestation d'un militant, affirme que ce genre de tactique annonce la nature des prochaines guerres : « This is cyberwar. The next Pearl Harbor. I was with the former head of the CIA two days ago and he said the next sneak attack is not coming from land or water, it is coming from cyberspace » (Hunt et MacFarland, 2010). L'analogie avec Pearl Harbor évoque un symbole collectif significatif de la Deuxième Guerre mondiale et place de ce fait les individus militant sous la bannière d'Anonymous comme des ennemis du mode de vie américain.

Les prochains paragraphes exposeront la manière dont sont vulgarisées les tactiques d'Anonymous dans le discours des médias. Les sections vouées à définir les actions par déni de service représentent une partie très importante des extraits codés dans le corpus de documents médiatiques. Il sera tout d'abord argumenté que les informations concernant le fonctionnement technique du LOIC, les impacts des mobilisations ainsi que la masse de participants requise pour ralentir un site ou le mettre hors service divergent d'un article à l'autre. Nous analyserons ensuite de

quelles manières, dans une perspective plus globale, les stratégies discursives mises de l'avant dans les discours des médias délégitiment les hacktivistes en évacuant partiellement la notion de militance.

4.2.2.3 Les actions par déni de service dans les médias

Alors que les termes « distributed denial of service attack », son abréviation (DDoS) ainsi que le nom du logiciel LOIC sont utilisés dans la quasi-totalité des articles, il n'en reste pas moins peu d'entre eux expliquent la nature de l'action technique comme étant une attaque envers des sites web sans fournir d'explications techniques supplémentaires. Ces articles en notent tout de même son caractère illégal. Ainsi, si une majorité d'entre eux élabore de manière plus exhaustive sur ce que constitue une action par déni de service et décrit celle-ci comme l'action « to flood websites with huge amounts of Internet traffic to shut hem down » (Fox News, 2010e), le reste du corpus reste truffé de contradictions relatives à l'impact direct des actions, à la facilité d'utilisation du LOIC et de la masse de participants prenant part aux mobilisations.

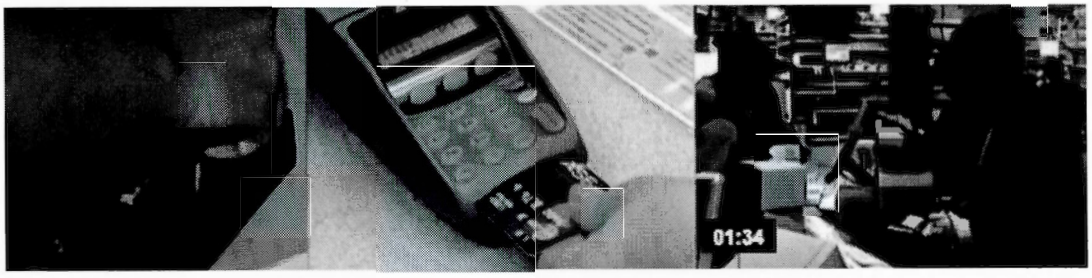
Les actions par déni de service sont présentées dans le discours d'Anonymous comme des protestations symboliques ne visant pas à atteindre d'infrastructures critiques. Cette notion n'est abordée qu'une fois dans le discours des médias qui avancent que « the attacks don't appear to be meant to do more than create a show, [...] the hackers don't seem to be seeking confidential company or consumer information » (Dwyer, 2010). Effectivement, la majorité des articles associent cette tactique à des pratiques éminemment perturbatrices (Constanza-Chock, 2003), notamment en soutenant que l'objectif de celle-ci est de « bring down a website by hitting it with an overwhelming number of simultaneous requests of information » (Fox News, 2010e) de manière à les mettre hors ligne ou à ralentir leurs opérations, « thus denying service to legitimate users » (Ryan, 2011a).

Bien que plusieurs articles notent que les données personnelles des consommateurs et les services relatifs à l'usage et au paiement des cartes de crédit ne sont pas affectés, une minorité d'entre eux soulignent que seulement les sites corporatifs sont ciblés par les attaques (FoxNews, 2010a ; Fox News, 2010b ; Housh, 2011). Ainsi, si le corpus s'avère unanime sur le fait que les actions ralentissent ou mettent des pages web hors-ligne, il est néanmoins moins clair sur ce qui détermine l'impact sur le consommateur. Le fait que les consommateurs ne soient pas mis à risque n'est pas attribué aux décisions stratégiques d'Anonymous, permettant de rattacher la « sécurité » des consommateurs aux mesures déployées par les corporations.

Dans cet ordre d'idées, le visuel utilisé dans une quinzaine de reportages projette l'image que les informations de cartes crédit ainsi que l'habileté d'utiliser les cartes sont compromises par les actions d'Anonymous. Effectivement, les images ci-bas issues du reportage « Anonymous' Hackers High Profile Targets » diffusé sur les ondes d'ABC présentent de multiples cartes de crédit à découvert, vulnérables au vol.

4.5 Cartes de crédit (Sciutto, 2010)

Les images suivantes, issues du reportage "Operation Payback Wages War Online", mettent en scène différents consommateurs utilisant leurs cartes de crédit dans des commerces.



4.6 Cartes de crédit (Fox News, 2010d)

Le reportage "Wiki-War: Operation Payback", quant à lui, présente comme image d'ouverture, le logo de Wikileaks ainsi qu'un terminal affichant la mention « declined ». Ces exemples suggèrent que les actions d'Anonymous aient un impact sur l'usage des cartes de crédit, alimentant une peur relative aux répercussions des mobilisations : « when you're talking about the Internet, hackers and credit cards, all that in the same sentence, it's a little bit enerving, especially during the holiday season » (Shuetter, 2011).

Il est important de noter qu'aucun article ne traite des « dommages » concrets infligés aux sites web visés par les tactiques ni des pertes financières potentiellement occasionnées par celles-ci. Par contre, plusieurs articles soulignent dûment l'illégalité de l'action, en avançant quelles actions enfreignent le « Computer Fraud and Abuse Act » et que les militants peuvent être poursuivis au civil et au criminel pour « conspiring to intentionally cause damage to protected computers » (Stark et Muir, 2012 ; Ryan, 2011a ; Frieden et Candiotti, 2011 ; Fox News, 2010b ; Fox News Associated Press, 2011 ; Gordon, 2011a).

4.2.2.4 Cadrage du LOIC

Tout d'abord, plusieurs articles notent la simplicité d'utilisation du logiciel LOIC (Dwyer, 2010 ; ABC News, 2011 ; FoxNews, 2010a ; Fox News, 2010e ; Rasch et

Todd, 2010 ; CNN Writer Staff, 2010 ; Frantz et Schubert, 2010 ; Shuetter, 2011), permettant à des « ordinary people to participate on targeted assault on websites » (FoxNews, 2010a). Cette description s'avère contradictoire à l'image véhiculée dans d'autres articles où la représentation des mobilisations techniques est accompagnée d'images de fils entremêlés d'ordinateurs et de codes binaires. De plus, de nombreux articles, omettant de nommer le LOIC, font référence aux actions par déni de service comme étant des « hack attacks » (Smith, 2010 ; Dwyer, 2010 ; FoxNews, 2010a ; Fox News, 2010d). Dans tous les cas, il est possible de noter une divergence entre la description des mobilisations techniques, qui, pour la plupart, sont qualifiées d'attaques ou de *hacks,* les explications techniques entourant l'usage facile du LOIC et les éléments visuels accompagnant les descriptions narratives.

Le LOIC est également présenté, dans quelques articles, comme un outil permettant de joindre un botnet de manière volontaire (Frantz et Schubert, 2010 ; Housh, 2011 ; Fox News, 2010b ; Fox News, 2010e). Alors que seulement six articles expliquent ce que constitue techniquement un botnet (Dwyer, 2010 ; Frantz et Schubert, 2010 ; Gross, 2011 ; Housh, 2011 ; Fox News, 2010b ; Fox News, 2010e), quatre d'entre eux soutiennent que les ordinateurs peuvent être involontairement infectés dans l'objectif de mener une attaque. Ainsi, l'utilisation de botnets tend à délégitimer les mobilisations d'Anonymous : « The truth is the actual attack is not coming from those few individuals [...] They're commanding an extremely broad network of computers being controlled by whatever the puppetmaster wants them to do » (Dwyer, 2010). En ce sens, l'usage des technologies numériques à des fins militantes est perçu comme un multiplicateur de forces qui, selon certains journalistes, démontre que « in this super networked world, there is a very few number of people that can have an outsized effect » (Sciutto, 2010). La tactique tend également à être associée

au *slacktivisme*[40] ainsi qu'à l'image de l'adolescent, cette fois-ci, présenté comme paresseux: « This group of people has grown frustrated with trying to protest [...] they've finally figured out they can use technology to fight back, that they don't have to stand in a picket line » (Fox News, 2010e).

Finalement, la notion de masse est mobilisée pour décrire le nombre de personnes ainsi que la force de frappe requise pour mener à bien une action par déni de service. Ce nombre varie grandement d'un article à l'autre. Effectivement, pour interrompre le service d'un site web d'une grande corporation (tel que Visa, par exemple), le nombre d'ordinateurs varie, selon les articles, entre 120 ordinateurs (Frantz et Schubert, 2010) jusqu'à plusieurs milliers (Fox News, 2010e). Bref, il va sans dire que l'information relative aux actions techniques d'Anonymous dans l'*Operation : Payback* est très peu étoffée et diverge grandement d'un article à l'autre. De manière plus générale, les articles tendent à mettre l'accent sur la nature illégale de l'action, sans pour autant expliquer les impacts directs (techniques et financiers) entraînés par l'interruption d'un site web corporatif. Dans les rares occasions où la question de la masse est mobilisée, l'usage de technologies numériques dans un contexte de militance délégitime les mobilisations, soit par l'usage de botnets involontaires – opposant donc la notion de masse d'information à celle de la masse d'individus mobilisés —, soit par l'usage de botnets volontaires – associant les mobilisations à du *slacktivisme.*

4.2.3 La menace hacktiviste

Les différentes techniques discursives mises de l'avant dans le discours des médias tendent à évacuer les enjeux éthiques et politiques mis de l'avant par les militants

[40] Le « slacktivisme » est un mot-valise signifiant, en français, « activisme paresseux ». Effectivement il joint les mots anglais « slacker » et « activism ».

pour n'aborder leurs tactiques qu'en fonction de leurs implications juridiques. Les brèves allusions à la désobéissance civile électronique et aux problématiques émanent du MVDA (Jordan, 2002) construisent le schème d'une menace. Alors que nous avons noté à quelques reprises que l'image des militants et leurs actions techniques soient associées à celle du *hacker*, l'usage de la technologie dans un contexte de militance semble être perçue comme quelque chose de menaçant parce que difficile à prévoir. À ce titre, les propos de Hafner et Markoff pour décrire les *hackers* des années 1980 semblent toujours être appropriés pour décrire les hacktivistes *:* « It's not surprising that parents, federal investigators, prosecutors and judges often panic when confronted with something they believe is too complicated to understand » (Hafner et Markoff, 1992, p. 11). Il n'est donc pas surprenant que la description des dimensions inhérentes aux pratiques hacktivistes menées dans l'*Operation : Payback* soit fréquemment rattachée à des enjeux d'ordre sécuritaire.

Ces enjeux sont également fortement mobilisés dans la description des actions techniques, particulièrement en ce qui a trait à la dimension de la non-violence. En effet, si plusieurs articles omettent de mentionner la nature violente ou non violente des mobilisations actuelles, ils notent cependant la potentialité violente véhiculée dans les mobilisations hacktivistes. Tel que rapporté dans l'article "The Top Four Cyber Threats for 2011":

> [H]acktivism can turn into something less like a peaceful protest and more like a riot. Politically motivated attacks also pose a greater threat if combined with StuxNet-level sophistication [...] It can move a little beyond just taking down a web site [...], and into actually weaponized attacks with the goal to cause real-world damage (ABC News, 2011).

Dans le même ordre d'idées, Brad Garrett note, dans le reportage « Anonymous Hacker's High Profile Targets » que « the big concern is they do have the where of all

to do destructive damage to national security, to corporations, and even to indviduals. » (Stark et Muir, 2012) Ces stratégies discursives visent à élaborer le schème d'une menace en mettant l'accent, de manière plus importante, sur l'illégalité de ces actions, sur leur caractère malicieux (ABC News, 2011 ; Frantz et Schubert, 2010 ; Fox News, 2010d) puis sur les menaces que de telles formes de militance représentent envers les infrastructures critiques et l'intégrité physique des individus.

CHAPITRE 5 : DISCUSSION

5.1 Retour sur les sous-questions et les résultats de la recherche

Les résultats tirés de l'analyse de discours opérée sur les trente-quatre documents du corpus médiatique et les neuf diffusés par le collectif nous permettent de répondre aux quatre sous-questions de recherches posées. En premier lieu, le collectif est cadré dans le discours des médias américains comme un réseau sombre et mystérieux dont la structure organisationnelle décentralisée et secrète rend presque impossible la tâche d'identifier les individus prenant part aux opérations ni de connaître leur nombre exact. Ce discours décrédibilise la notion selon laquelle ces individus seraient des militants; ceux-ci étant surtout définis comme des supporteurs de Wikileaks ou comme des hackers. Les militants, quant à eux, construisent dans leur discours une image inclusive d'Anonymous qui, basée sur l'anonymat des participants, permettrait un mode de gestion basé sur les idées plutôt que sur les dirigeants, promouvant de ce fait une image très perméable des valeurs pouvant être portées dans différentes mobilisations. Cette identité de justiciers du cyberespace, avant tout basée sur le fait que tout le monde peut être Anonymous, est construite directement sur l'identification de l'Autre, c'est-à-dire des acteurs corrompus et n'agissant pas au nom du bien commun.

En deuxième lieu, l'opération est cadrée dans le discours des médias comme une réaction plutôt émotive à des événements politiquement et légalement justifiables. Les revendications des militants sont présentées comme étant des opinions parmi d'autres, évacuant donc leur caractère politique et les normes éthiques mobilisées.

Les pratiques techniques sont également délégitimées à travers de nombreux processus discursifs (souvent contradictoires), c'est-à-dire par l'illégalité de l'action par déni de service, par l'association de cette tactique au *slacktivisme*, par le rapprochement sémantique à des actes de *hacking* pouvant donner lieu à des attaques plus graves dans le futur ou par la mobilisation de botnets involontaires – délégitimant la notion de masse et renforçant l'image du *hacker* criminel. Pour les militants, l'opération n'est pas légitimée à travers les processus techniques (i.e masse de participants versus masse d'information) mis en place, mais par l'aspect symbolique et les valeurs portées à travers la mobilisation (pas d'atteinte à des infrastructures critiques, objectif de publicité, valeurs présentées comme défendant le bien commun).

Ensuite, les revendications politiques et les pratiques du collectif transgressent les codes techniques de l'environnement stratégique néolibéral de plusieurs manières. Premièrement, par la conceptualisation du cyberespace comme d'un endroit propice à la mobilisation. Cette conceptualisation donne lieu à de nombreuses pratiques transgressives. Parmi celles-ci, les actions par déni de service – considérées comme un siège électronique – et l'utilisation des réseaux numériques comme lieu permettant la communication tactique – les IRC étant perçus comme transgressifs par leur caractère secret et l'utilisation des réseaux sociaux tels que Facebook et Twitter étant présentés comme non réglementaires (par la suspension des comptes des militants pour cause de « non-respect des conditions d'utilisation »). Ensuite, la notion de l'anonymat et de l'effacement de l'individu derrière la collectivité, dans l'ensemble des pratiques du collectif, défie les codes de l'environnement stratégique, ne serait-ce que par le manque de transparence du collectif aux yeux des médias, complexifiant les pratiques de surveillance et rendant de ce fait le groupe imprévisible. Finalement, les valeurs et revendications relèvent de la transgression, des politiques contentieuses

de Tarrow, dans la mesure où les demandes ne peuvent être satisfaites dans le contexte sociopolitique actuel.

Dans cette mesure, que le discours des médias supporte leur cadrage du collectif et de l'opération en mettant de l'avant des enjeux majoritairement d'ordre juridique et sécuritaire. Alors que l'enjeu d'ordre juridique permet de mettre l'accent sur les valeurs illégales promues par le collectif (i.e le piratage de matériel protégé) ainsi que sur leur tactique principale (actions par déni de service), les enjeux d'ordre sécuritaires sont rattachés au fait que le collectif supporte les principes de Wikileaks, mais surtout à la menace potentielle qu'ils représentent. Effectivement, les champs lexicaux reliés à la guerre ainsi que l'image du *hacker* permettent de dresser le schème d'une menace pouvant semer le chaos sur l'Internet (Hunt et MacFarland, 2010), voire même atteindre l'intégrité physique des individus. Cela se pose en contradiction complète avec le discours véhiculé par Anonymous. Ce dernier met plutôt de l'avant des enjeux éthiques en se basant sur l'universalité des valeurs présentées pour supporter le cadrage de ses mobilisations et de son identité. Il pose néanmoins ces valeurs en tant qu'adversité antagoniste avec l'environnement stratégique néolibéral dans la mesure où l'usage du champ lexical de la guerre est surtout utilisé pour interpeler directement ceux qui sont perçus comme les *ennemis* du collectif ou pour dénoncer des pratiques jugées comme immorales.

À la lumière de ces résultats, il sera question d'aborder comment les discours des médias de masse américains et ceux des militants participent à la production du sujet (Foucault, 1976) hacktiviste. Nous analyserons ensuite comment ils mettent en scène des rapports s'exerçant autant dans des formes de micropouvoir que dans des rapports de pouvoir *macros* s'inscrivant dans des dynamiques sociales plus globales. Nous soutiendrons que ces mobilisations révèlent un lien clair entre les notions de la tactique telle que conceptualisée par de Certeau et de l'affrontement des stratégies tel

que défini par Foucault. Autrement dit, les pratiques tactiques des militants donnent lieu à des affrontements stratégiques opérés à travers le discours.

De cette manière, nous verrons comment d'une part, les discours rendent compte des pratiques tactiques des militants et, d'une autre part, comment le caractère transgressif de ces tactiques et les luttes sémantiques entourant leur cadrage relèvent de l'affrontement des stratégies. Plus précisément, nous soutiendrons qu'alors que les mobilisations d'Anonymous sont définies comme éminemment transgressives et que celles-ci défient plusieurs codes techniques de l'environnement stratégique néolibéral, leurs processus organisationnels reflètent et (re)produisent les dynamiques sociales inhérentes au système-monde.

5.2 L'affrontement des stratégies: une mutation de l'hyperindividualisme?

Les valeurs véhiculées à travers les discours d'Anonymous visent à exposer des pratiques de corruption inhérentes au mode de gouvernance néolibéral. Effectivement, les *Anons* tendent à qualifier d'illégitimes les pratiques opérées par les décideurs politiques notamment par la mise en valeur des principes de la liberté de l'information, de la liberté d'expression, des libertés individuelles et de la méfiance envers l'autorité. Ainsi, il serait juste de dire que les principes éthiques véhiculés par Anonymous et identifiés dans les discours des médias entretiennent de nombreux points communs avec les principes fondamentaux du libéralisme. Il est donc possible d'associer les valeurs soulevées dans les deux discours à celles mises de l'avant par les *hackers* du mouvement « Free and Open Source Software » (F/OSS). Celles-ci constituent, selon Coleman, « a liberal critique within liberalism » (Coleman, 2012, p. 2) :

> [H]ackers [...] extend as well as reformulate key liberal ideals such as access, free speech, transparency, equal opportunity, publicity and meritocracy. [...] Hackers sit simultaneously at the center and margins of the liberal tradition.

> [...] As such, [...] [they] not only reveal a longstanding tension within liberal legal rights but also offer a targeted critique of the neoliberal drive to make propety out of almost anything (Coleman, 2012, p. 2-3).

Selon cette perspective, bien que plusieurs revendications d'Anonymous se posent en opposition à l'environnement stratégique néolibéral, il n'en reste pas moins que leur mode d'organisation décentralisé tend à la (re)production de ses dynamiques sociales en se rapprochant conceptuellement de plusieurs principes associés à l'éthique du *hacker* (Levy, 1985). Les *hackers,* par leur propension à valoriser la méritocratie et par leur dévouement au « productive freedom »[41] (Coleman, 2012) semblent accorder une plus grande importance au fonctionnement optimal d'un objet technique qu'aux rapports politico-idéologiques transcendantaux qu'il véhicule. Ainsi, toute forme de restriction technique peut être perçue comme une entrave à la liberté personnelle des *hackers* et à leur capacité de modifier un programme ou un logiciel à leur gré.

Dans cette mesure, les pratiques de *hacking* peuvent s'apparenter à ce que Mondoux conceptualise comme l'hyperindividualisme, c'est-à-dire à l'individu advenant par et pour lui-même en se distanciant par la même occasion de toute forme d'autorité. Selon cette perspective, il est pertinent de noter que l'association de l'image du hacktiviste à celle du *hacker* dans le discours des médias et que la manière dont est mobilisée la notion de l'individualisme dans le discours d'Anonymous permettent une redéfinition de la notion d'hyperindividualisme dans un contexte de militance politique.

---

[41] Selon Gabriella Coleman, le terme « [productive freedom] designates the institutions, legal devices and moral codes that *hackers* have built in order to autonomously improve on their peers work, refine their technical skills and extend craftlike engineering tradition » (Coleman, 2012, p.3).

5.2.1 L'anonymat et l'hyperindividualisme dans le discours des militants

Le discours d'Anonymous s'inscrit dans cette forme d'hyperindividualisme notamment à travers son organisation décentralisée et la perméabilité idéologique de ses mobilisations, participant de cette manière à une certaine occultation du politique. Effectivement, l'anonymat est présenté dans le discours des militants comme une force transgressive et est mobilisé pour former une identité collective antagoniste à celle du système-monde. De cette manière, si nous avons soutenu dans les derniers paragraphes qu'Anonymous opérait à travers une réinterprétation de plusieurs principes libéraux, il sera ici argumenté que la notion de l'anonymat permet une redéfinition de l'hyperindividualisme, reflétant donc des relations de pouvoir relatives, d'une part, aux hacktivistes transgressant les codes techniques de l'environnement stratégique néolibéral et, d'une autre part, à la nécessité de ceux-ci à (re)produire plusieurs processus organisationnels inhérents à ce même environnement.

Tel qu'abordé précédemment, l'hyperindividu ne tend pas à s'extérioriser du système-monde puisque ce dernier lui permettrait de se réaliser pleinement en jouissant de libertés individuelles. Cependant, il importe de se questionner sur la réaction de l'hyperindividu lorsque les pratiques de gouvernance nuisent à sa capacité de jouir de ses libertés individuelles (i.e partager des fichiers ou de l'information). De nombreuses valeurs mises de l'avant dans les discours d'Anonymous et soulevées dans le discours des médias (tel que la méfiance envers l'autorité, la liberté d'expression, etc.) peuvent se rattacher à la notion de l'hyperindividualisme. Pourtant, la prédominance du « je » au profit du « nous » et la dépolitisation de la sphère publique pour l'atteinte de la jouissance personnelle (Mondoux, 2011) semble contradictoire aux valeurs collectives et aux nombreux principes éthiques et politiques mis de l'avant dans le discours d'Anonymous. C'est pourquoi nous

avançons que la politisation de l'hyperindividu, entraîné par une certaine suppression de ses libertés individuelles, peut aisément donner lieu à un collectif prenant cette forme décentralisée.

Effectivement, la perméabilité idéologique et la décentralisation de l'organisation peuvent aisément interpeler l'hyperindividu à s'impliquer dans des mobilisations lui permettant de militer ponctuellement autour d'une cause touchant ses intérêts personnels. Cela va de pair avec les résultats d'une recherche menée par Molly Sauter qui constate l'impact biographique des mobilisations d'Anonymous sur les militants dans l'*Operation : Payback*:

> [T]he subsomption of personal agency has the potential for a strong biographical impact on the participants, particularly, those who had not previously considered themselves political actors. It allowed those who had considered themsleves to be an audience in the world of politics and industry to become actors, strengthened by the invisible yet palpable presence of thousands of their new comrades-in-arms (Sauter, 2013, p. 998).

Dans le même ordre d'idées, si la notion de l'anonymat est intrinsèquement liée dans le discours d'Anonymous à la capacité de mobiliser des masses de militants autour d'enjeux différents, elle revêt également d'un caractère symbolique par le fait qu'elle transgresse des codes relatifs à la transparence des individus dans le système-monde. Elle permet de ce fait l'effacement de l'individu au profit de la collectivité et se pose en tant que front uni contre une série d'adversaires et ce, malgré les disparités idéologiques à l'interne du collectif. La notion de l'anonymat permet au collectif de se poser en tant que force unie et transgressive et elle rend possible sa perméabilité idéologique qui garantit une capacité à se porter garant des libertés individuelles et collectives face à un ennemi commun défini comme corrompu. Selon cette perspective, l'anonymat et l'individuation des pratiques militantes, exposées à travers l'absence de projet idéologique explicite et transcendant, semblent être mobilisés dans le discours des militants comme une condition nécessaire pour échapper à la surveillance totale du monde numérique et de l'environnement stratégique néolibéral.

Ainsi, Anonymous tend à désorbiter ses pratiques en se proclamant comme un groupe de justiciers du cyberespace reniant toute affiliation idéologique explicite et agissant en réaction à des conjonctures ponctuelles. Pourtant, cette absence de projet idéologique transcendant ne signifie pas que les pratiques transgressives du collectif sont dépourvues de leur caractère politique. Celles-ci visent plutôt à ramener le politique (Mouffe, 2005) dans un discours néolibéral se définissant comme ontologique. Dit autrement, si les processus organisationnels (re)produisent les dynamiques sociales inhérentes au système-monde, leurs valeurs et leur esthétisme visent à repositionner le discours néolibéral comme une production symbolique et non comme une ontologie.

5.2.2 *Hacking*, hacktivisme et individualisme dans les médias

Dans cet ordre d'idées, le discours des médias tend à désorbiter les mouvements tactiques (de Certeau, 1990), c'est-à-dire à individualiser les pratiques marginales pouvant se rattacher à une adversité antagoniste en les privant de leur caractère politique. Effectivement, la configuration idéologique néolibérale conceptualisée à travers le système-monde (Mondoux, 2011) favorise la production de sujets individuels diversifiés. Ce dernier, en incluant les subjectivités dans son environnement stratégique et en leur donnant l'impression de se réaliser pleinement à travers, entre autres, la jouissance de libertés individuelles, vise à transformer toute adversité antagoniste en adversité agoniste (Mouffe, 2005). Les pratiques marginales et individuelles se muent donc en « mouvement brownien de tactiques invisibles et innombrables » (de Certeau, 1990, p. 66) dans un environnement stratégique conçu pour régner dans la diversité.

En ce sens, l'association entre le hacktiviste et le *hacker* est symptomatique de cette tendance discursive à désorbiter les mouvements tactiques. Si l'image du *hacker* ainsi

que ses pratiques peuvent être associées à une utilisation tactique des technologies, il n'en reste pas moins que celles-ci sont individualisées, extériorisées (via la criminalité) ou intégrées au système par le discours des médias. À ce titre, notons que l'ancien *hacker* de renommée internationale, Kevin Mitnick, agit en tant qu'intervenant dans l'un des reportages et est présenté non pas comme un ancien *hacker*, mais comme l'auteur du livre « Ghost in Wires » et comme un expert en sécurité informatique. Le discours médiatique extériorise donc les *hackers* du système-monde en rattachant leurs actions à une forme de criminalité. Sinon, il ignore les activités illégales opérées par le passé, comme dans le cas de Mitnick, pour ne présenter que celles décrites comme légales donc légitimes.

Ainsi, le hacktiviste est présenté comme un individu cherchant soit à partager des fichiers de manière illégale, à se vanter de ses actions techniques ou à humilier les autorités publiques. Ses actions et ses motivations, quant à elles, sont associées à des opinions personnelles ou à des excès de rage plutôt qu'à des actions militantes. Sommairement, le discours des médias souligne le caractère illégal des mobilisations et individualise les pratiques hacktivistes pour les cadrer comme des actes dépourvus de caractère politique, comme des tactiques désorbitées et invisibles.

5.2.3 L'occultation du politique

L'affrontement des stratégies s'opère donc dans le discours des médias à travers leur manière de cadrer Anonymous comme une extériorité au système-monde, que ce soit par la nature illégale de leurs actions techniques ou la menace potentielle pour l'ordre en place qu'il représente. D'entrée de jeu, l'occultation du politique s'exerce dans le discours des médias par la délégitimation globale des principes éthiques mis de l'avant par le collectif. Celle-ci s'opère à travers l'évacuation fréquente de la notion de militance dans la description des mobilisations et du collectif dans son ensemble;

ensuite par le rattachement des actions par déni de service et de leurs impacts à des principes légaux et sécuritaires; puis, finalement, par la présentation des militants comme des individus irrationnels – ces derniers étant rattachés à l'image de l'adolescent *hacker* s'adonnant périodiquement à des excès de rage et devant être *socialisé*. L'image du sujet hacktiviste est donc construite autour de son irrationalité et de la criminalité de ses actions et soutenue par des enjeux d'ordre juridique et sécuritaire permettant l'évacuation du politique.

Ainsi, l'occultation du caractère politique de l'*Operation : Payback* témoigne de la tendance du système-monde à présenter son discours comme non idéologique. Le discours ne se présente donc pas comme une production symbolique, mais comme une ontologie. Les principes légaux et les codes techniques mis de l'avant dans ce dernier servent à titre de référence pour juger de la légitimité des actions et de leur moralité. Ils apparaissent comme une finalité en soi, notamment par le fait que les attaques soient qualifiées par la loi comme d'une *conspiration* envers des ordinateurs protégés et par l'association de l'illégalité des attaques avec un caractère malicieux.

En deuxième lieu, il importe de noter, encore une fois, la propension qu'on les médias à désorbiter les tactiques du collectif dans leurs discours relatifs à l'*Operation : Payback*. Effectivement, les médias accordent certainement un plus grand intérêt à cadrer les individus prenant part aux mobilisations plutôt que de comprendre le collectif dans son ensemble. Ainsi, en cadrant les discours politiques comme des opinions personnelles et en dépolitisant le sujet en le plaçant dans des catégories ontologiques claires (Mondoux, 2011) – c'est-à-dire en le cadrant comme un être présocial ou comme un criminel – la stratégie discursive des médias rend difficile, voire impossible, l'émergence du politique dans le discours hacktiviste.

5.2.3.1 Le schème d'une menace

L'occultation du politique est finalement renforcée par les processus discursifs qui présentent Anonymous comme une menace pour l'ordre en place. Cette menace est perceptible à travers les nombreux enjeux sécuritaires soulevés dans la description du collectif et de ses mobilisations. Il est pertinent de noter que les enjeux sécuritaires sont uniquement basés sur les risques d'une transposition dans le cyberespace des actions politiquement motivées. Effectivement, les énoncés rattachés à ces enjeux décrivent faussement les impacts des mobilisations (notons, à titre d'exemple, les nombreuses images de cartes de crédit exposées, laissant donc supposer que la capacité des citoyens à consommer et à se servir de leurs cartes de crédit serait restreinte par les actions par déni de services d'Anonymous), ou amplifient les connaissances techniques de militants. Ces amplifications et simplifications permettent de supposer que de subséquentes « attaques » pourraient avoir un impact beaucoup plus grave sur les activités quotidiennes des citoyens, sur le bon fonctionnement du système-monde et pourraient même atteindre l'intégrité physique des individus. De cette manière, les pratiques d'Anonymous sont sémantiquement liées aux cyberguerres et, implicitement, au cyberterrorisme et, par extension, à la notion de terrorisme post 11 septembre. Effectivement, si cette dernière association n'est jamais mentionnée dans le corpus, il n'en reste pas moins qu'il est possible de rattacher la description que font les médias du groupe décentralisé, mystérieux, secret et fâché contre les grandes corporations américaines, à une menace terroriste.

Finalement, le discours des médias délégitime le discours et les actions politique d' Anonymous à travers la description du caractère imprévisible des actions du collectif, véhiculé par son manque de transparence, par la mauvaise compréhension de ses actions techniques et de leurs impacts. Ainsi, l'objectivation (Foucault, 1990) des

militants comme des criminels, comme d'une menace au système, permet à ce discours d'occulter le caractère politique du collectif en deux temps : premièrement, en dissociant les pratiques collectives pour les cadrer comme des mouvements tactiques «innombrables et invisibles » (de Certeau, 1990, p. 66) puis en cadrant ces mouvements comme une forme de criminalité. Ces stratégies permettent aux médias de dessiner implicitement les limites du système-monde et de placer les hacktivistes en son extérieur. Ainsi, si l'extérieur du système-monde est conceptualisé, dans le discours des militants, comme une adversité antagoniste, le discours néolibéral renie cette possibilité. Effectivement, l'absence d'adversité antagoniste est constitutive de ce discours (Mouffe, 2005) et celui-ci tend plutôt à présenter l'antagonisme comme une adversité agoniste ou comme une extériorité claire, représenté par la criminalité et par la menace envers la sécurité nationale.

5.3 Un ennemi qui vous veut du bien

Alors que les pratiques tactiques, telles que le doxing, la communication sur les IRC et les actions par déni de service, ont été utilisées dans d'autres contextes, le fait que ces dernières soient utilisées dans le cadre d'une mobilisation rassemblant une masse – plus ou moins importante – de militants donne nécessairement lieu à des rapports de pouvoir. Effectivement, ces rapports de pouvoir se forment lorsque des tactiques se rassemblent autour d'une identité, d'une voix et de valeurs communes. Ainsi, bien que les deux discours placent Anonymous dans un rapport transgressif au système-monde, l'affrontement des stratégies s'opère alors que l'un vise à se positionner en tant qu'adversité antagoniste (Mouffe, 2005) et que l'autre tend à l'extérioriser du système-monde en le rattachant à une menace pour l'ordre en place. Bref, ces affrontements stratégiques prennent forme à travers l'innovation dans le répertoire d'actions militantes et dans diverses stratégies de répressions (Tarrow, 2010) mises en place dans le système-monde (Mondoux, 2011).

5.3.1 Le cyberespace comme objet et outil de militance

L'affrontement des stratégies s'opère donc majoritairement dans le discours des militants autour de la défense de l'intérêt commun et de la conceptualisation du cyberespace comme d'un espace propice à la mobilisation. Ces deux notions sont centrales dans le discours du collectif. Le corpus de ce dernier accorde une grande importance à la définition des valeurs idéologiques et organisationnelles, aux finalités des mobilisations et à l'identification claire des adversaires — dont les intérêts, bien que défendus par les institutions étatiques et juridiques, ne relèvent pas du bien commun.

La conceptualisation du cyberespace comme objet et outil de militance permet au collectif de poser ses actions et ses valeurs éthiques en opposition aux codes techniques mis de l'avant par l'environnement stratégique néolibéral. Ces codes techniques sont rattachés à ce que Jodi Dean conceptualise comme le capitalisme communicationnel, c'est-à-dire à la matérialisation des idéaux néolibéraux dans les TIC. Effectivement alors que le collectif reconnaît que l'Internet est d'abord un lieu marchand, le discours de ses militants est axé sur des revendications politiques et des pratiques techniques qui remettent en questions ces codes et leur pertinence sociale et politique. Cette remise en question est opérée discursivement à la fois autour de la nécessité de changement radical des valeurs structurant l'Internet ainsi que par la possibilité d'utiliser les technologies numériques comme outil de militance. Le discours d'Anonymous est de ce fait orienté autour de la conceptualisation d'un Internet neutre et permettant le partage de matériel et d'information à travers les communautés. Les technologies numériques sont donc défendues comme étant un vecteur de progrès social plutôt que de profit économique.

De cette manière, l'affrontement des stratégies a lieu dans la manière de conceptualiser et d'utiliser le cyberespace. En effet, selon Foucault, l'affrontement

des stratégies est lié à l'objectif d'agir sur « un adversaire de telle manière que la lutte soit pour lui impossible » (Foucault, 1978, p. 1042). Ainsi, le discours des médias met de l'avant des enjeux juridiques et sécuritaires pour légitimer la criminalisation des hacktivistes afin de protéger les codes techniques structurant le cyberespace. Les militants, pour leur part, cadrent les codes techniques du cyberespace comme injustes et légitiment leur discours autour de la promotion de nouveaux codes qui profiteraient au plus grand nombre. Dans ces conjonctures particulières, les militants promeuvent de nouveaux codes relatifs, entre autres, à la gouvernance du cyberespace en le conceptualisant — par l'utilisation et le détournement de logiciels pour restreindre l'adversaire dans des protestations symboliques — non pas comme un lieu d'échange commercial, mais comme un espace social propice à des mobilisations politiques. La comparaison avec les mouvements sociaux des années 1960 illustre efficacement cet argument : si, dans ces années, les militants bloquaient des banques et des commerces dans le cadre de protestations non violentes, alors dans le contexte sociotechnique actuel, il serait légitime de protester sur les plateformes numériques.

5.3.2 La notion de masse

Conséquemment, la défense des intérêts individuels et collectifs est directement associée avec la notion de masse. Le collectif légitime ses mobilisations non pas à travers le nombre d'individus prenant part à celles-ci, mais plutôt par rapport à la portée globale des valeurs diffusées dans l'espace public. Effectivement l'usage de botnets non volontaires ne semble pas être perçu comme une pratique illégitime par le collectif, bien que plusieurs la définissent comme éthiquement douteuse (Coleman, 2014; Sauter, 2013; Olson, 2012). Plutôt, la multiplicité des militants mobilisés dans une variété de tactiques (en opposition à une masse de participants mobilisés dans une action par déni de service), doublés des finalités de la mobilisation permet aux protestations d'être légitimées en fonction de l'impact symbolique (publicité) et du caractère global des valeurs qu'elles supportent.

5.3.3 L'identification de l'adversaire

Enfin, les stratégies discursives exposées dans les documents du collectif visent à dénoncer les pratiques de corruption, c'est-à-dire qu'elles ont pour objectif de démontrer comment les structures juridiques, économiques et politiques ne défendent plus les intérêts du plus grand nombre de citoyens. Dans cette mesure, le discours d'Anonymous déconstruit les arguments de ceux qu'ils perçoivent comme des ennemis et expose les contradictions inhérentes au discours néolibéral. À ce titre, Foucault note que les rapports de pouvoir sont induits, entre autres, par l'objectivation du sujet, c'est-à-dire par le fait que « le sujet est soit divisé à l'intérieur de lui-même, soit divisé par les autres » (Foucault, 1982, p. 1042) — donnant lieu à une catégorisation entre, par exemple, le fou et le sain d'esprit ou entre le criminel et le « bon garçon ». Cela se rattache à l'identification de l'Autre dans les travaux de Chantal Mouffe (2005). Ainsi, si les militants sont objectivés dans le discours des médias comme des criminels, le processus inverse est également opéré par Anonymous dans ses pratiques discursives. Effectivement, l'identification de l'adversaire est cruciale dans les stratégies discursives du collectif qui visent à distancier cette figure du criminel en dissociant les notions d'éthique et de légalité.

Selon cette perspective, même si les fondements des principes éthiques des militants se rattachent à l'environnement stratégique néolibéral, il n'en reste pas moins que l'identification claire des adversaires et des principes injustes qu'ils défendent sert à l'édification d'une adversité antagoniste. Celle-ci est opérée par les pratiques discursives et par les politiques contentieuses (Tarrow, 2010) des militants visant à une mutation des codes de l'environnement stratégique et, donc, à des changements d'ordre culturels (Costanza-Chock, 2003).

5.3.4 Conclusion partielle

En somme, l'affrontement des stratégies est abordé par Anonymous à travers la mise en valeur de principes éthiques et politiques. Même si les valeurs mises de l'avant par le collectif peuvent être liées à certains principes libéraux, il n'en reste pas moins que celles-ci ne sont pas posées comme des valeurs réformistes au système en place. La transgression se démarque par sa capacité à ramener le politique (Mouffe, 2005) dans un discours libéral qui l'avait effacé. Finalement, et de manière cohérente avec la vision de la tactique de Michel de Certeau, l'affrontement des stratégies tel que véhiculé dans les pratiques discursives du collectif prend la forme de ce que Foucault qualifie de stratégie de lutte (Foucault, 1982) : « la stratégie de lutte constitue elle aussi une frontière : celle où l'induction calculée des conduites chez les autres ne peut aller au-delà de la réplique à leur propre action » (Foucault, 1982, p.1061). Il est ainsi possible de rapprocher conceptuellement les « strategies of struggle » (Foucault, 1978) au collectif contentieux de Tarrow et à la tactique (de Certeau, 1990).

5.4 La tactique dans les mobilisations d'Anonymous

Nous argumenterons dans les prochains paragraphes que les discours véhiculés par les médias et les militants placent les pratiques d'Anonymous comme relevant de la tactique, notamment à travers le caractère réactionnaire du collectif, son organisation secrète et par son fonctionnement décentralisé.

5.4.1 Un collectif contentieux

En premier lieu, la structure décentralisée du collectif peut être associée à la tactique. Comme noté par Tarrow, un mouvement contentieux – à la différence d'un collectif – est défini à partir de la globalité de ses actions et de sa capacité « [to] build

organizations, [to] elaborate ideologies and socialize and mobilize constituencies » (Tarrow, 2010, Empl. 508). Effectivement, même si Anonymous entretient des valeurs éthiques claires, sa perméabilité idéologique et son caractère réactif permettent de noter l'absence d'un projet global. Dans cette optique, il ne relève pas d'un mouvement qui aurait la possibilité d'établir un environnement stratégique distinct, mais plutôt d'un collectif et de la tactique par son impossibilité « de se donner un projet global ni de totaliser l'adversaire dans un espace distinct, visible et objectivable » (de Certeau, 1990, p. 61). La notion de temporalité est, dans cette mesure, cruciale à l'élaboration des actions militantes du collectif. Effectivement, l'identification des adversaires et des causes portées par Anonymous est faite en réaction à des conjonctures particulières.

5.4.2 « L'art des faibles » et l'habile utilisation du temps

Par le fait que les mobilisations d'Anonymous sont majoritairement motivées par « a collective sense of being fed up with all the minor and major injustices we witness everyday » (Anonymous Anarchy, 2010) et par le positionnement du collectif comme un groupe de justiciers du cyberespace, il va sans dire que ses tactiques relèvent, pour reprendre les termes de de Certeau, de « l'art du faible » visant à « rendre plus forte la position la plus faible » (de Certeau, 1990, p. 62). Anonymous défendrait dans ses actions les intérêts des sous-représentés par les institutions politiques et législatives. Effectivement, les codes techniques mis en place dans le système-monde sont opposés à ceux mis de l'avant dans les mobilisations. Ainsi, puisque les principes éthiques véhiculés par le collectif ne sont pas défendus dans les institutions actuelles, alors les pratiques employées pour les défendre sont donc exercées par les faibles.

Dans cette optique, la présentation du caractère réactionnaire d'Anonymous se rattache également à la notion de tactique. Effectivement, puisque l'*Operation : Payback* a été déclenchée à la suite un ensemble de conjonctures particulières, ses

pratiques sont liées à la tactique dans la mesure où elles « visent à une habile utilisation du temps; des occasions qu'il présente et aussi des jeux qu'il introduit dans les formations du pouvoir » (de Certeau, 1999, p. 63). Cette habile utilisation du temps est en relation directe avec l'objectif de publicité présenté dans les discours d'Anonymous et dans ceux des médias – cet objectif étant atteint, notamment, par des actions militantes à caractère symbolique. Cela est cohérent avec ce qui est avancé par Gabriella Coleman dans l'article « The Power Behind the Mask » : « Anonymous tends to ride and amplify the wave of existing events or causes. [...] Sometimes, Anonymous misses the wave, especially when the mainstream media fails to jump on board to report on its operations » (Coleman, 2014, p. 3). Si, dans le cas de l'*Operation : Payback*, il est juste de dire qu'Anonymous a réussi à attirer l'attention des médias, il n'en reste pas moins que ce mode de fonctionnement relève indubitablement de la tactique dans la mesure où la réussite de la mobilisation dépend de la publicité qu'elle génère. Conséquemment, elle repose sur le *momentum* créé à la fois par le contexte dans lequel s'ancre la mobilisation et par les pratiques militantes du collectif capables d'instrumentaliser les médias et de tirer avantage d'une situation.

Ainsi, si les objectifs des mobilisations sont atteints par l'habile utilisation du temps et des conjonctures sociales, économiques et politiques, alors les actions techniques relèvent d'une utilisation tactique des technologies numériques de l'environnement stratégique néolibéral : elles utilisent « les failles, que les conjonctures particulières ouvrent dans la surveillance du pouvoir propriétaire, elle[s] y braconne[nt] » (de Certeau, 1990, p. 63). Effectivement, que ce soit par l'utilisation des IRC ou du LOIC, Anonymous tente de se dérober[42] à la surveillance inhérente au système-monde en usant de modes de communication secrets et souvent encryptés pour

[42] Tel que noté dans la présentation du cas, les *script kiddies* impliqués dans l'*Operation Payback* n'étaient pas en mesure de remarquer comment l'architecture technique du LOIC ne protégeait pas leur identité lors des manifestations. Cette conjoncture a mené à l'arrestation de nombreux militants.

coordonner ses mobilisations et en utilisant des outils détournés de leurs fonctions originales pour mener à bien leurs pratiques militantes. De cette manière, le mode de communication secret via les IRC relèverait d'un « mouvement dans le champ de vision de l'ennemi » (de Certeau, 1990, p. 61). Le LOIC, tel que relevé dans l'article « We Want You, Say Hacktivists… but Is it Legal ? », est, quant à lui, décrit comme un outil développé par des experts en cybersécurité pour tester la résistance des sites web au trafic numérique. Ce programme disponible en « open source » a donc été modifié en outil de mobilisation. Ce détournement peut donc être associé au parallèle qu'établit de Certeau entre la langue et la parole. Effectivement, si la langue relève de la stratégie par le fait qu'elle impose des structures, des règles grammaticales, etc. la parole, quant à elle, relève de la tactique puisqu'elle donne à la langue des tournures inattendues (de Certeau, 1990; Feenberg, 2002).

CONCLUSION

Le présent mémoire s'intéressait aux nouveaux répertoires d'actions militantes (Tarrow, 2010) que représentent les mobilisations hacktivistes. Le hacktivisme est abordé à la fois comme une innovation technique dans les pratiques de militance et comme étant symptomatique de nouveaux enjeux liés à la gouvernance des technologies numériques. Dans cette mesure, nous nous sommes questionnés sur les rapports de pouvoir inhérents à ces nouvelles pratiques à travers le cas spécifique de l'*Operation : Payback* menée par le collectif Anonymous. Cette recherche a accordé une importance particulière au contexte sociotechnique dans lequel ces rapports de pouvoir prennent place ainsi qu'à l'influence qu'a eue la production historique du sujet (Foucault, 1982) hacker sur la construction actuelle de l'image du hacktiviste.

Effectivement, l'appropriation des technologies numériques par des groupes de militants se fait dans un contexte où les TIC et les informations qu'elles génèrent sont grandement liés aux pratiques gouvernances (Mattelart, 2010). Une revue de la littérature nous a ainsi permis de comprendre les TIC comme porteuses de valeurs politiques, sociales et économiques (Dean, 2003; Dean, 2009; Nissembaum, 2004) tout en étant utilisées pour rationaliser et légitimer les pratiques de gouvernance prétendument non idéologiques dans le système-monde (Feenberg, 2004; Freitag, 2008; Mondoux, 2011). L'environnement stratégique (de Certeau, 1990) devient donc un lieu d'identification et de construction d'un discours néolibéral autour de valeurs qualifiées d'universelles. À ce titre, l'architecture du cyberespace et les valeurs qu'il supporte visent avant tout à protéger les intérêts du libre marché (Dean,

2003) par l'usage de dispositifs à la fois techniques et juridiques (Lessig, 2003) qui posent le fonctionnement des réseaux comme neutre et rationnel, représentant ainsi une ontologie sociale (Nissenbaum, 2004). Cette ontologie sociale permet donc l'édification des valeurs identitaires d'un environnement qui a comme dimension constitutive de son hégémonie, l'absence d'adversité antagoniste (Mouffe, 2005).

Dans ce contexte, le *hacker,* faisant autrefois figure d'innovation et de virtuosité technique, se mue rapidement en un hors-la-loi, en un pirate ou en un criminel dont les actions imprévisibles deviennent un danger pour les infrastructures critiques (Levy, 1984; Hafner & Markoff, 1995; Conway, 2009). De manière plus importante, cette image permet d'associer tout usage détourné ou non permis des TIC à une menace potentielle pour l'ordre en place; cadrant de ce fait le *hacker* comme une extériorité au système-monde. Ainsi, l'identification des sujets en fonction de l'illégalité de leurs actes techniques – et non en fonction des motivations ou des finalités de leurs pratiques – mène conséquemment à une confusion conceptuelle entre les différents répertoires d'actions utilisant des techniques de *hacking.* Tel que noté par plusieurs auteurs, cet élargissement donne lieu à des luttes sémantiques liées au cadrage des mobilisations hacktivistes : certains acteurs visent ainsi à conceptualiser ces pratiques émergentes comme des modes de protestations légitimes alors que d'autres tendent à les rapprocher d'actes de cyberterrorisme (Costanza-Chock, 2003; Conway, 2007, 2009).

La recherche visait principalement à analyser la manière dont les discours véhiculent et mettent en scène des rapports de pouvoir relatifs à la fois à l'usage tactique des technologies numériques et à la transposition des pratiques de militance dans le cyberespace (Jordan, 2004). Ces rapports n'ont pas été compris comme une forme de pouvoir s'exerçant depuis une série d'institutions envers une série d'acteurs dominés, mais plutôt comme des « relations entre partenaire [s] » (Foucault, 1982, p. 1053), c'est-à-dire en termes de relations complexes s'exerçant tant aux niveaux micro que

macro (Foucault, 1982). Cette recherche s'est donc opérationnalisée à travers l'étude et la comparaison des discours produits par les médias de masse américains (corpus de 34 articles) et par les militants (corpus de neuf articles), ceux-ci participant à la construction de la figure du hacktiviste et de ses actions de militance dans l'imaginaire populaire.

Ce choix méthodologique, d'abord motivé par l'absence de littérature traitant des luttes sémantiques liées à la conceptualisation des militants et des mobilisations hacktivistes, tenait pour acquis qu'il y avait un écart entre les deux discours à l'étude. Dans cette optique, les objectifs principaux visaient à aborder les enjeux autour desquels s'articulent ces écarts de conceptualisation, de manière à utiliser les formes de résistance « comme un catalyseur [...] qui permet de mettre en évidence les relations de pouvoir, de voir où elles s'inscrivent, de découvrir leurs points d'application et les méthodes qu'elles utilisent » (Foucault, 1982, p. 1044); à voir comment est problématisée la transposition des pratiques militantes sur les technologies numériques à travers le MVDA; et, finalement, à explorer comment ces relations de pouvoir révèlent des enjeux idéologiques sous-jacents à l'usage tactique des technologies numériques.

Nous avons donc identifié dans les discours à l'étude la manière dont étaient cadrés les militants et l'*Operation : Payback*, les enjeux éthiques, juridiques, politiques, économiques et sécuritaires mobilisés pour soutenir les différents cadrages ainsi que les codes techniques inhérents à l'environnement stratégique néolibéral défiés par les pratiques hacktivistes. De cette manière, les résultats de la recherche peuvent sommairement se résumer par la constatation que les deux types de discours s'intéressaient à des thématiques et à des enjeux différents.

Premièrement, les discours d'Anonymous visent surtout à légitimer leurs pratiques de militance en mettant de l'avant presque uniquement des enjeux d'ordre éthique. Ceux-ci servent à établir une image rassembleuse et positive du collectif en tant que défenseurs du peuple. À cet effet, ces principes servent à identifier l'adversaire, l'Autre (Mouffe, 2005) comme un ennemi corrompu. De cette manière, les pratiques du collectif transgressent délibérément plusieurs valeurs supportées par le discours néolibéral. Premièrement, elles transgressent explicitement les codes techniques relatifs à la gouvernance du cyberespace par le cadrage de leurs actions comme une forme de désobéissance civile électronique et par les principes politiques défendus dans les mobilisations (i. e partage de fichiers protégés). Ensuite, l'esthétisme prônant l'anonymat des participants et la structure organisationnelle décentralisée, tous deux visant l'inclusion d'un maximum de participants et le renforcement de l'image selon laquelle tout le monde peut devenir Anonymous, transgressent implicitement les codes d'un environnement stratégique où la surveillance et la transparence des individus relèvent d'un enjeu primordial à l'exercice de la gouvernance.

L'anonymat, le caractère décentralisé du collectif ainsi que l'usage de *techniques de hacking* dans les mobilisations est davantage utilisé dans le discours des médias pour peindre une image opaque et potentiellement menaçante des hacktivistes. Effectivement, en mettant de l'avant des enjeux, pour la plupart, d'ordre juridique et sécuritaire, ce discours vise à individualiser les pratiques hacktivistes : le collectif reste très peu abordé dans son ensemble, l'on tente surtout de qualifier les individus prenant part aux mobilisations en associant la plupart du temps leurs connaissances techniques à celles des *hackers*; les finalités et les motivations sont fréquemment évacuées au profit de brèves descriptions des actes techniques et, surtout, de leur nature illégale; finalement, de nombreux articles mettent implicitement ou explicitement en perspective les manières selon lesquelles le hacktivisme a autant le potentiel de nuire aux pratiques de consommation quotidiennes que de devenir une menace pour la sécurité nationale.

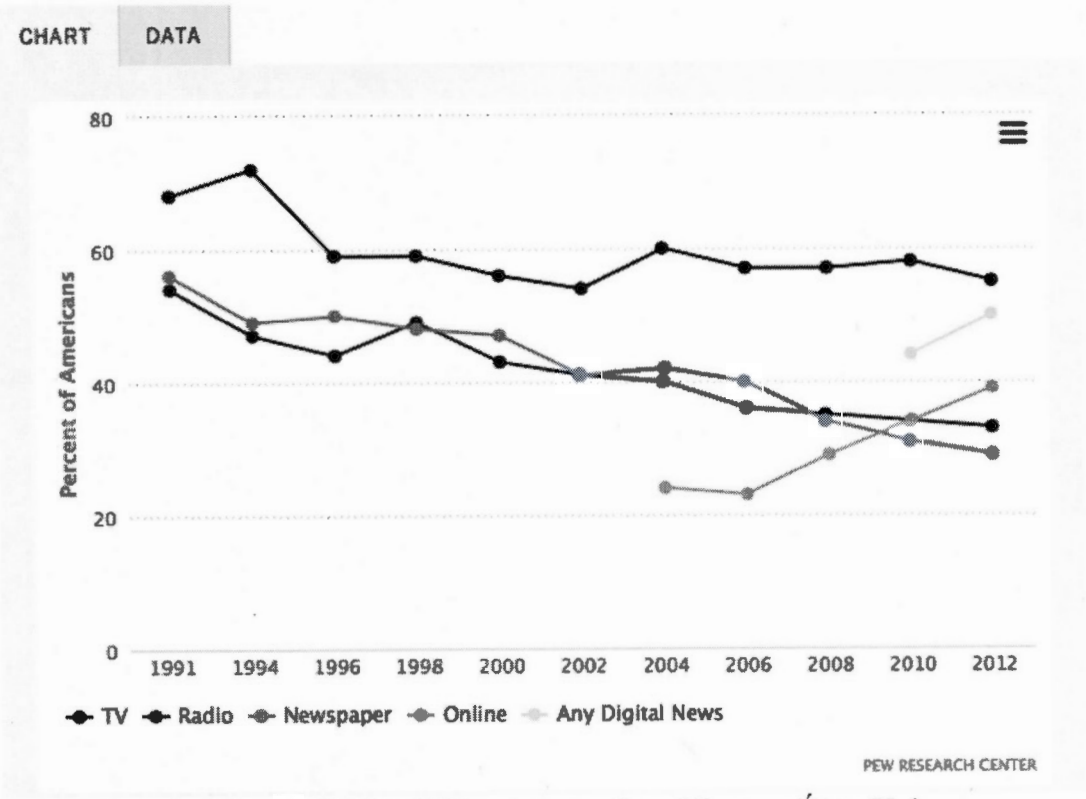
En regard des résultats de recherche obtenus, les rapports de pouvoir induits par les mobilisations hacktivistes entourant l'*Opertation Payback* se situent principalement en ce qui a trait à l'occultation du politique. L'occultation du politique est perceptible majoritairement à travers l'individualisation des pratiques militantes. Celle-ci est abordée dans chacun des discours, mais selon des perspectives divergentes. Alors que les médias tendent à marginaliser les pratiques militantes en évacuant leur caractère politique à travers de nombreuses stratégies discursives – positionnant donc le discours relatif à l'environnement stratégique néolibéral comme ontologique –, les pratiques et le discours d'Anonymous utilisent plutôt cette individuation afin de créer une image de justicier du cyberespace.

Effectivement, la perméabilité idéologique est au cœur de l'identité et des valeurs esthétiques et organisationnelles portées par le collectif. Selon cette perspective, il serait facile de rattacher les pratiques d'Anonymous à des mouvements tactiques dispersés et dénués de sens politique global, tel que soutenu dans le discours des médias. Cependant, nous croyons que cette apparente occultation du politique à travers la décentralisation du collectif ainsi que la notion de l'anonymat permettent plutôt au collectif de se dérober de la surveillance totale inhérente au système-monde – rendant de ce fait ses actions imprévisibles, donc transgressives. Dans cette mesure, nous avançons qu'Anonymous émerge et se rattache au terrain et au contexte processuel lié au système-monde en (re)produisant certaines de ces dynamiques sociales, mais qu'il permette également une remise en question et une transgression drastique de nombreux codes techniques liés à cet environnement. Autrement dit, l'occultation du politique majoritairement lié aux processus organisationnels du collectif résultant en l'absence d'un projet idéologique transcendant ne signifie pas pour autant qu'Anonymous n'est pas *politique.* Tel que relevé par Tarrow, puisque la forme du collectif ne permet pas de projet idéologique global, Anonymous se trouve donc contraint à des « stratégies de luttes » (Foucault, 1982), à agir en réaction à des

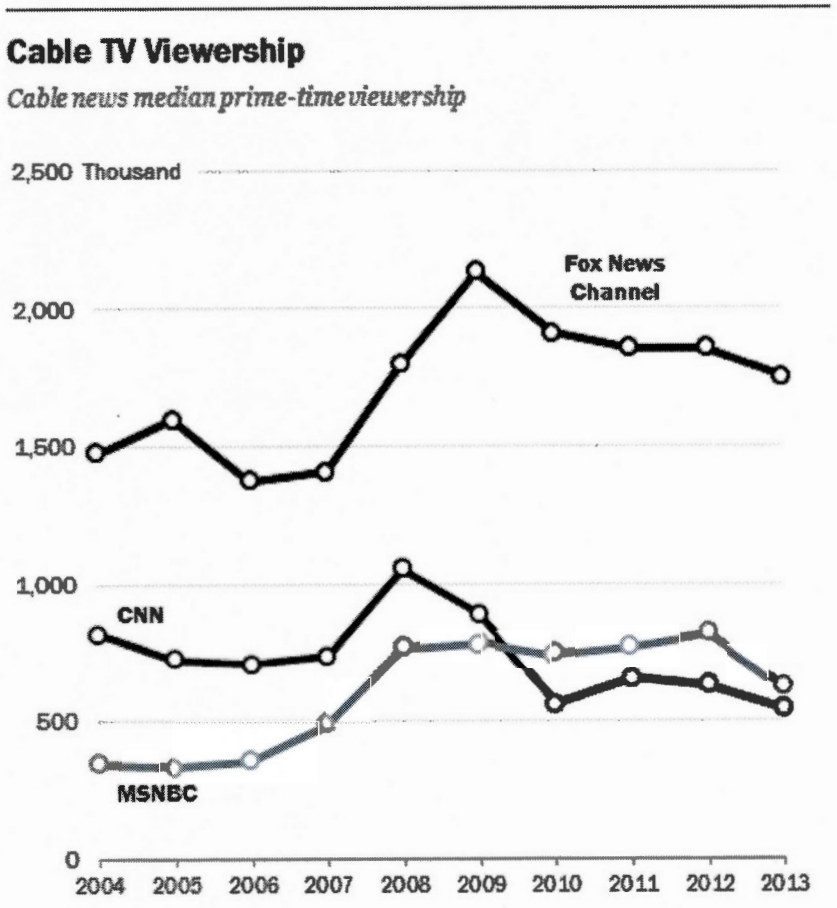
conjonctures particulières et à faire appel à des tactiques (de Certeau, 1990) pour se dérober aux pratiques de gouvernance et pour transgresser leurs codes techniques dans l'objectif éventuel d'atteindre des changements d'ordre culturels (Costanza-Chock, 2003).

Finalement, il est nécessaire de noter deux limites incontournables à l'analyse de discours effectuée dans cette recherche. En premier lieu, notons que la majorité des articles du corpus médiatique ont été publiés dans les deux jours ayant suivi les actions par déni de service contre Visa, MasterCard et PayPal (voir annexe E). Ainsi, les articles du corpus semblent avoir été écrits, enregistrés et diffusés sans enquêtes de fond préalable, entrainant de ce fait un certain sensationnalisme et un manque potentiel de nuances dans l'analyse des mobilisations. En deuxième lieu, la perméabilité idéologique d'Anonymous ainsi que son caractère réactif rend délicate la généralisation des résultats obtenus à l'ensemble des mobilisations hacktivistes. De cette manière, s'il avait été noté que la recherche qualitative inductive visait à généraliser les résultats de l'étude de l'*Operation : Payback*, certains de ces résultats ont démontré qu'il serait sans doute nécessaire de comparer les discours produits dans plusieurs mobilisations, c'est-à-dire dans diverses coupes synchroniques du discours (Jäger et Maier, 2009). Effectivement, une recherche traitant et comparant les discours générés dans plusieurs mobilisations du collectif nous permettrait de pallier à ces deux limites.

ANNEXE A : CONSOMMATION DES NOUVELLES AUX ÉTATS-UNIS



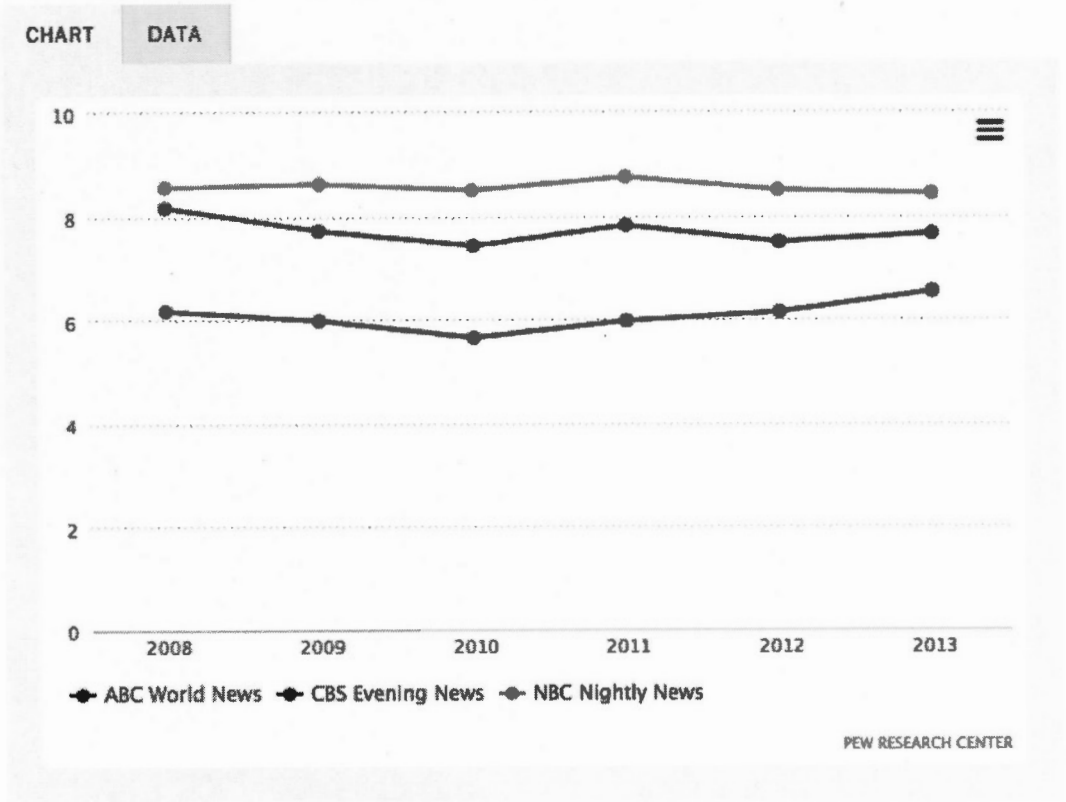
A .1 Popularité des différents types de médias aux États-Unis



A.2 « Cable TV Viewership »

Evening News Viewership by Network

Year-to-Year Average Viewers per Night in Millions



A.3 Cotes d'écoute des réseaux de nouvelles

ANNEXE B : ARTICLES DU CORPUS DE DOCUMENTS MÉDIATIQUES

Date de diffusion	Notice bibliographique	Citation courte	Codage Nvivo
2010	Sciutto, J. (2010) Wikileaks Crackdown Prompts Cyber Attacks. ABC News. [Reportage vidéo en ligne] Récupéré de http://abcnews.go.com/International/wikileaks-cyberattacks-fbi-executes-40-search-warrants-us/story?id=12782171	Sciutto, 2010	ABC1
08—déc-10	Pham, S. (2010, 8 décembre). Exclusive: Sarah Palin Under Cyber-Attack from Wikileaks Supporters in "Operation Payback". ABCNews. [Article en ligne] Récupéré de http://abcnews.go.com/blogs/politics/2010/12/exclusive-palin-under-cyber-attack-from-wikileaks-supporters-in-operation-payback/	Pham, 2010	ABC2
09—déc-10	Sciutto, J., Ferran, Lee et Goldman, R. (2010, 9 décembre). Lawyer: Assange Accusers 'Treated Like Perpetrators'. ABC News. [Article en ligne] Récupéré de http://abcnews.go.com/US/operation-payback-anonymous-cyber-battle-erupts-wikileaks/story?id=12351428&page=2	Sciutto et coll., 2010	ABC3
10—déc-10	Dwyer, D. (2010, 10 décembre). Foot Soldiers for Wikileaks: 27,000 Download Attack Software Overnight. ABC News. [Article en ligne] Récupéré de http://abcnews.go.com/Technology/wikileaks-anonymous-cyber-attacks/story?id=12355960	Dwyer, 2010	ABC4
07—janv-11	Non précisé (2011, 7 janvier). The Top Four Cyber Threats for 2011. ABC News. [Article en ligne] Récupéré de http://abcnews.go.com/Blotter/cyber-threats-2011-age-stuxnet-hacktivists-social-spammers/story?id=12555830	ABC News, 2011	ABC5

27—janv-11	Ryan, J. (2011, 27 janvier). Wikileaks Cyberattacks : FBI Executes More Than 40 Search Warrants Across US. ABC News. Récupéré de http://abcnews.go.com/International/wikileaks-cyberattacks-fbi-executes-40-search-warrants-us/story?id=12782171	Ryan, 2011a	ABC6
19—juil-11	Wolfe, B. (2011, 19 juillet). Anonymous hackers Arrested by FBI. ABC News.[Article en ligne] Récupéré de http://abcnews.go.com/blogs/politics/2011/07/anonymous-hakcers-arrested-by-fbi-wikileaks-operation-payback-assange/	Wolfe, 2011	ABC7
20—juil-11	Sy, S. (2011, 20 juillet). Hackers Arrest: More than a Dozen Suspects. ABC News. [Article en ligne] Récupéré de http://abcnews.go.com/WNT/video/abc-news-update-14118047	Sy, 2011	ABC8
13—déc-11	Ryan, J. (2011, 13 décembre). FBI Arrests 'Anonymous' Member for Attack Against GeneSimmons.com. ABC News.[Article en ligne] Récupéré de http://abcnews.go.com/blogs/politics/2011/12/fbi-arrests-anonymous-member-for-attack-against-genesimmons-com/	Ryan 2011b	ABC9
02—mai-12	Stark, L. et Muir, D (2012, 2 mai). Anonymous Hacker's High Profile Targets. ABC News. [Reportage vidéo en ligne]. Récupéré de http://abcnews.go.com/WNT/video/anonymous-hackers-high-profile-targets-governments-businesses-cyber-threat-technology-15518717	Stark et Muir, 2012	ABC10
17—juil-12	McDermott, Q. (2012, 17 juillet). 'Operation Payback' accused says he has no regrets. ABC News. [Article en ligne] Récupéré de http://www.abc.net.au/news/2012-06-18/anonymous-four-corners/4077476	McDermott, 2012	ABC11
08—déc-10	Bouldon, J. (2010, 8 décembre). 'Operation Payback' fuels cyberwar. CNN. [Reportage vidéo en ligne] Récupéré de www.cnn.com/video/data/business/2010/12/08/qmb.boulden.operation.payback.cnn.html	Bouldon, 2010	CNN1

08—déc-10	Rasch, M et Todd, M. (2010, 8 décembre). CNN's Briand Todd investigates claims that Visa and MasterCard are under cyber attack from supporters of Julian Assange. CNN. [Reportage vidéo en ligne] Récupéré de www.cnn.com/2010/US/12/09/hackers.wikileaks	Rasch et Todd, 2010	CNN2
08—déc-10	Schubert, A. (2010, 8 décembre). Hacker 'activists' target Mastercard. CNN. [Reportage vidéo en ligne] Récupéré de http://www.cnn.com/2010/US/12/09/hackers.wikileaks/	Schubert, 2010	CNN3
08—déc-10	Smith, A. (2010, 8 décembre). MasterCard, Visa targeted in apparent cyberattack.CNN. [Article en ligne] Récupéré de http://money.cnn.com/2010/12/08/news/companies/mastercard_wiki/	Smith, 2010	CNN4
09—déc-10	CNN Writer Staff (2010, 9 décembre). Pro-WikiLeaks hackers change target to PayPal. CNN. [Article en ligne] Récupéré dehttp://www.cnn.com/2010/WORLD/europe/12/09/world.wikileaks/	CNN Writer Staff, 2010	CNN5
10—déc-10	Shuetter, J.(2010, 10 décembre). Explain it to me: Cyber attacks. CNN. [Reportage vidéo en ligne]Récupéré de www.cnn.com/2010/US/12/09/hacker.wikileaks	Shuetter, 2010	CNN6
10—déc-10	Fantz, A. et Schubert, A. (2010, 10 décembre). WikiLeaks 'Anonymous' hackers: 'We will fight'. CNN. [Article en ligne] Récupéré de http://www.cnn.com/2010/US/12/09/hackers.wikileaks/	Frantz et Schubert, 2010	CNN7
20—juil-11	Frieden, T et Candiotti, S. (2011, 20 juillet). 14 hackers arrested in operation targeting Anonymous. CNN. [Article en ligne] Récupéré de http://www.cnn.com/2011/CRIME/07/19/new.york.anonymous.warrants/index.html?iref=allsearch	Frieden et Candiotti, 2011	CNN8
27—juil-11	Gross, J.(2011, 27 juillet). Hacker group urges boycott of PayPal. CNN. [Article en ligne] Récupéré de http://www.cnn.com/2011/TECH/web/07/27/anonymous.paypal.message/index.html?iref=allsearch	Gross, 2011	CNN9

10—août-11	Housh, G. (2011, 10 août). Gregg Housh explains the ideology of the group 'Anonymous'. CNN. [Reportage vidéo en ligne] Récupéré de http://www.cnn.com/2010/US/12/09/hackers.wikileaks/	Housh, 2011	CNN10
09—déc-11	Schuetter, J. (2011, 9 décembre). How far will Wikileaks Cyber war go?. CNN. [Reportage vidéo en ligne] Récupéré de http://www.cnn.com/2010/WORLD/europe/12/09/world.wikileaks/	Shuetter, 2011	CNN11
08—déc-10	Fox News.com (2010, 8 décembre). Hackers Target WikiLeaks 'Enemies': Mastercard, Twitter, Paypal, Even FoxNews.com. Fox News. [Article en ligne] Récupéré de http://www.foxnews.com/tech/2010/12/08/wikileaks-supporters-launch-hack-attacks/	FoxNews, 2010a	FOX1
08—déc-10	Fox News Associated Press (2010, 8 décembre). Wikileaks Supporters Launch Cyber Attack on Palin. Fox News. [Article en ligne] Récupéré de http://www.foxnews.com/politics/2010/12/08/sarah-palins-website-attacked-wikileaks-supporters/?intcmp=related	Fox News Associated Press, 2010	FOX2
09—déc-10	Fox News (2010, 9 décembre). Cyber-Skirmishes, Street Protests, Rage Over WikiLeaks. Fox News. [Article en ligne] Récupéré de http://www.foxnews.com/tech/2010/12/09/wikileaks-supporters-launch-cyber-attack-amazon/?intcmp=related	Fox News, 2010b	FOX3
09—déc-10	Fox News (2010, 9 décembre). Facebook, Twitter Delete Pro-WikiLeaks Hackers' Account. Fox News. [Article en ligne] Récupéré de http://www.foxbusiness.com/markets/2010/12/09/facebook-twitter-delete-pro-wikileaks-hackers-account/	Fox News, 2010c	FOX4
09—déc-10	Fox News (2010, 9 décembre). Operation Payback Wages War Online. Fox News. [Reportage vidéo en ligne] Récupéré dehttp://video.foxnews.com/v/4453739/operation-payback-wages-war-online/#sp=show-clips	Fox News, 2010d	FOX5

09—déc-10	Kaplan, J. (2010, 9 décembre). We Want YOU, Say Hacktivists … but Is It Legal? Fox News. [Article en ligne] Récupéré de http://www.foxnews.com/tech/2010/12/09/wikileaks-operation-payback-hacktivists-legal/	Kaplan, 2010	FOX6
09—déc-10	MacFarland, KT et Hunt R. (2010, 9 décembre). Wiki-War: Operation Payback. [Article en ligne] Récupéré de http://video.foxnews.com/v/4454282/wiki-war-operation-payback/#sp=show-clips	Hunt et MacFarland, 2010	FOX7
09—déc-10	Fox News (2010, 9 décembre). WikiLeaks 'Data War' Growing, Hacktivists Say. Fox News. [Article en ligne]. Récupéré de http://www.foxnews.com/tech/2010/12/09/wikileaks-data-war-growing-hacktivists-say/?intcmp=related	Fox News, 2010e	FOX8
03—oct-13	Fox News Associated Press (2013, 3 octobre).Grand jury indicts 13 members of Anonymous. Fox News. [Article en ligne] Récupéré de http://www.foxnews.com/tech/2013/10/03/grand-jury-indicts-13-members-anonymous/	Fox News Associated Press, 2011	FOX9
11—déc-10	Olderman, K. (2010, 10 décembre). News on Anonymous Operation Payback. MSNBC. [Reportage vidéo en ligne] Récupéré de https://www.youtube.com/watch?v=ye_F0w5nP5w	Olderman, 2010	MSNBC1
09—mars-11	Nightly News MSNBC.com (2011, 9 mars). Inside CyberWars. MSNBC. [Reportage Vidéo en ligne] Récupéré de https://www.youtube.com/watch?v=ueoxXAuFTsM	MSNBC News, 2011	MSNBC2
26—juil-11	Gordon, S. (2011, 26 juillet).FBI Raids Arlington House in Hacking Case. NBC News. [Article en ligne] Récupéré de http://www.nbcdfw.com/news/tech/FBI-Raids-Arlington-House-in-Hacking-Case-126151358.html	Gordon, 2011a	NBC1

26—juil-11	Gordon, S. (2011, 26 juillet). Arlington Home Raided in FBI Hacking Investigation. NBC News. [Article en ligne] Récupéré de http://www.nbcdfw.com/news/tech/Arlington_Home_Raided_in_FBI_Hacking_Investigation_Dallas-Fort_Worth-126157078.html	Gordon, 2011b	NBC2

B.1 Corpus des documents médiatiques

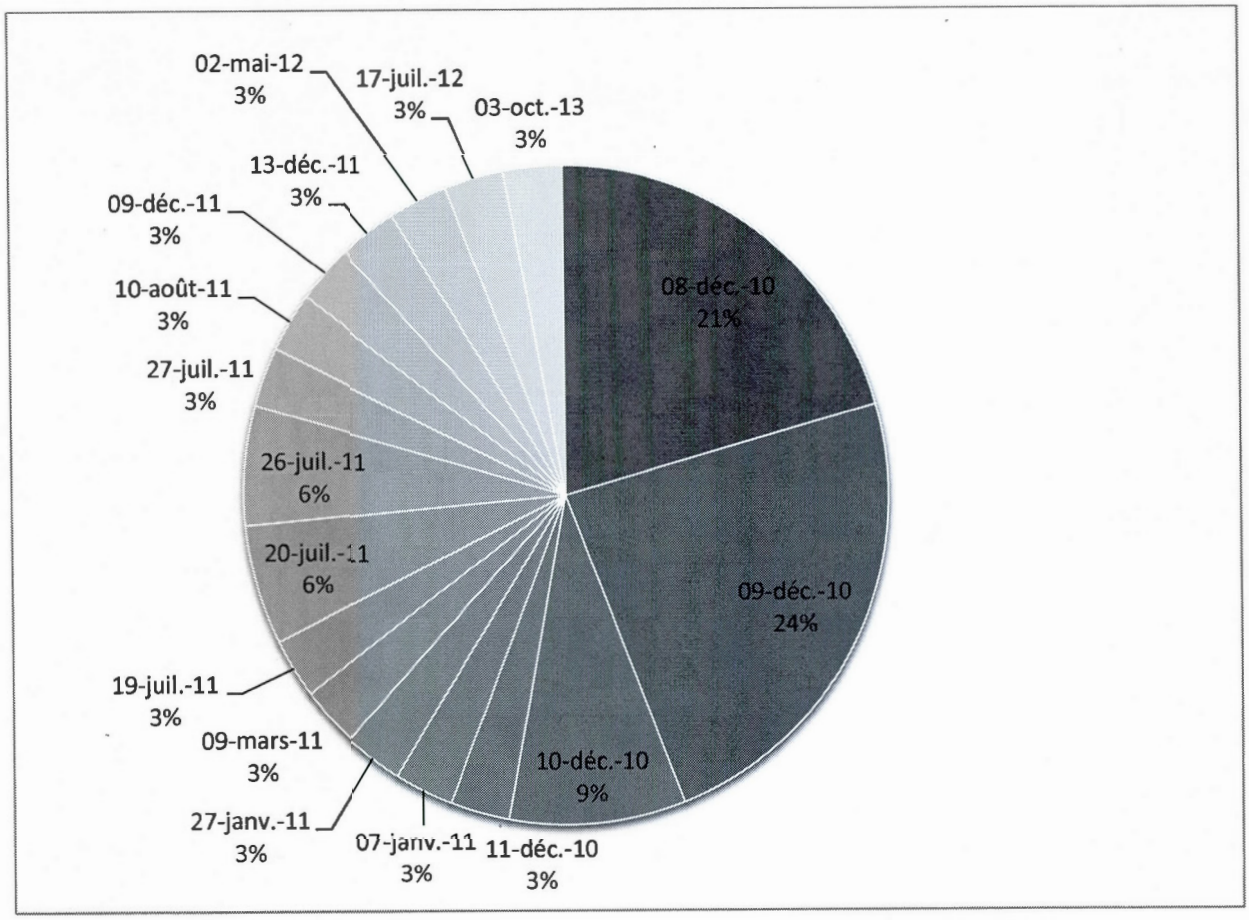
ANNEXE C : ARTICLES DU CORPUS DE DOCUMENTS PRODUITS PAR ANONYMOUS

Date de publication	Nombre de vues	Notice bibliographique	Référence courte	Codage NVivo
30 oct. 2010	310 870	Anonymous Anarchy (2010, 30 octobre). Operation Payback #Anonymous Message RE :ACTA, SOPA, PIPA, Internet Censorship & Copyright. [Vidéo]. Récupéré de https://www.youtube.com/watch?v=kZNDV4hGUGw	(Anonymous Anarchy, 2010)	Anon1
9 décembre 2010	245 114	A message from Anonymous (2010, 9 décembre) Our Message, Intentions and potential Targets. [Vidéo]. Récupéré de https://www.youtube.com/watch?v=WpwVfl3m32w	(A message from Anonymous, 2010)	Anon2
5 avril 2011	418 782	Alucar Ex (2011, 5 avril). ANONYMOUS – OPERATION PAYBACK – Sony Press Release. [Vidéo]. Récupéré de https://www.youtube.com/watch?v=2Tm7UKo4IBc	(Alucar Ex, 2011)	Anon3
11 décembre 2010	33 689	TheHairyHeart (2010, 11 décembre). ANON OPS : A Press Release : December 10, 2010. [Vidéo]. Récupéré de https://www.youtube.com/watch?v=fxT3Bn7_-Ig	(TheHairyHart, 2010)	Anon4

6 avril 2011	91 257	Anonymous6499 (2011, 6 avril). Anonymous : Second press release to Sony. [Vidéo] Récupéré de https://www.youtube.com/watch?v=eryqClObdO8	(Anonymous 6499, 2011)	Anon5
29 octobre 2010	28 261	Operation Payback (2010, 29 octobre). What is Operation : Payback ?. [Vidéo]. Récupéré de https://www.youtube.com/watch?v=Vp-wXWGRM18	(Operation Payback, 2010)	Anon6
Inconnue	Inconnu	Anonyme (2010a). Operation Avenge Assange. [Image et Texte]. Récupérée de http://knowyourmeme.com/photos/87085-operation-payback	(Anonyme, 2010a)	Anon7
Inconnue	Inconnu	Anonyme (2010b). Operation Payback Limewire. [Image et texte]. Récupéré de https://encyclopediadramatica.es/File:Operationpaybacklimewire.png	(Anonyme, 2010b)	Anon8
Inconnue	Inconnu	Anonyme (2010c). Operation Payback Gallant Macmillan. [Image et texte] Récupéré de https://encyclopediadramatica.es/File:Operation_Payback_GMlegal.png	(Anonyme, 2010c)	Anon9

C .2 Corpus des documents diffusés par Anonymous

ANNEXE D : DATES DE PUBLICATION DES ARTICLES DANS LE CORPUS DE DOCUMENTS MÉDIATIQUES



D.1 Dates de publication des documents du corpus médiatique

GLOSSAIRE

/b/board : Page du site 4chan.org aléatoire ou, en anglais, « random ». C'est sur cette page que circulent des discours dérangeants et des images violentes et obscènes; le contenu présenté sur la plateforme étant contrôlé de manière minimale par les administrateurs du site. C'est également sur cette plateforme qu'ont émergé les pratiques de trolling qui ont donné lieux au collectif Anonymous.

4chan.org : Site web composé de pages d'images mis en ligne le premier octobre 2003 où les utilisateurs publient sous le pseudonyme « Anonymous » des images ou des billets. Selon le fondateur, Christopher Poole, l'anonymat est un vecteur de créativité puisque les utilisateurs ne se censurent pas par peur de représailles.

Adresse IP : Il s'agit de l'adresse de protocole Internet qui est un numéro d'identification attribué de manière temporaire à un ordinateur.

Anon : Un individu prennant part aux activités d'Anonymous.

Action par déni de service : Une action par déni de service consiste au rechargement d'une page web à de multiples reprises par minute. L'envoi de paquets d'information provenant de plusieurs ordinateurs simultanément résulte souvent en un « blockage of public access to the target site (...). When targets are companies that rely on online sales, such actions can have significant economic as well as symbolic impact » (Costanza-Chock, 2003, p.6). Les actions par déni de service sont utilisées par des groupes de militants dans des actes de désobéissance civile électronique. Ces actions ne sont pas considérées comme du *hacking* vu la facilité de l'opération. Celles-ci sont pourtant illégales dans la majorité des jurisdictions.

Botmaster : Ordinateur contrôlant un botnet

Botnet : Provient des contractions des mots anglais "robots" et "réseaux". Un botnet est un logiciel capable d'infecter et de contrôler d'autres machines à distance à partir d'un centre de contrôle (Coleman, 2013). Les ordinateurs sont mobilisés par le téléchargement de virus, un vers, ou des chevaux trojans.

Botnet involontaire : Une série d'ordinateurs ayant téléchargé un virus, vers ou un cheval trojan de manière involontaire.

Botnet volontaire : Une série d'ordinateurs ayant téléchargé un virus, vers ou un cheval trojan de manière volontaire. Ces ordinateurs sont mobilisés, dans le cas qui nous intéresse, à envoyer des paquets d'information vers un serveur ciblé par le botmaster.

Doxing : Tactique parfois légale et parfois illégale qui consiste à rendre disponible des données personnelles et préférablement humiliantes de personnes ciblées. Cette tactique est fréquemment utilisée dans des campagnes de trolling. La légalité dépend de la protection des données exposées. À titre d'exemple, il est légal de publier des numéros de cartes de crédit, mais il est illégal de commettre des actes de fraudes avec ceux-ci et de "voler" ces donnée sur un ordinateur protégé.

Electro hippies : Groupe de militants altermondialistes qui ont utilisé les actions par déni de service pour bloquer l'accès aux sites du World Trade Organisation à Seattle en 1999.

Electronic Disturbance Theater : Un groupe de militants altermondialistes qui ont développé le FloodNet, programme permettant de faire de la désobéissance civile électronique.

FloodNet : Logiciel développé par le Electronic Disturbance Theater dans le contexte des protestations altermondialistes au Mexique dans les années 1990. Le FloodNet est conçu pour recharger automatiquement une page web sélectionnée par le groupe militant (et non par l'utilisateur) depuis un ordinateur. Le logiciel ne permet pas de joindre de botnets.

Internet Relay Chat : Les Internet Relay Chat (IRC) sont des sites web destinés au clavardage en temps réel. Un même site web peut héberger plusieurs conversations identifiées à l'aide du # (i.e #hacktivisme). Pour joindre une conversation, il s'agit donc de se diriger sur ledit site web et de rechercher la conversation voulue. Certaines conversations s'avère plus protégées et nécessitent de ce fait une invitation préalable d'un membre ou l'approbation du modérateur au moment de joindre le groupe.

Low Orbit Ion Canon : Logiciel open source utilisé par Anonymous pour mener les actions par déni de service. On fait souvent référence au logiciel de par son accronyme, LOIC.

Lulz : Découle de l'accronyme "lol" (Laught Out Loud) et est, entre autre, utilisé par les trolls sur 4chan pour signifier un humour dérangeant. Dit autrement,il est utilisé pour "express that one carried out a specific action for the sake of personal comic enjoyment. This is sometimes used to to explain why one has posted offensive, far-fetched or disgusting contents on image boards and discussion forums." (Know Your Meme, 2010).

Meme : Le terme a été utilisé pour la première fois en 1976 par le biologiste Richard Dawkins dans son livre "The selfish gene". Il représente une idée ou un comportement qui se répend de personnes en personnes. Depuis, le terme a été réapproprié par les usagers de l'Internet. Il s'agit majoritairement d'images accompagnées de texte qui "[spreads] virally [and leaps] from IP address to IP address (and brain to brain) via a process which, in the broad sense, can be called imitation". (Solon, 2013)

Open Source : Qualifie un logiciel dont le code source est disponible à l'utilisateur. Ce dernier est ainsi capable de modifier le logiciel ou le programme à sa guise.

Ordinateur zombies : Ordinateurs mobilisés dans un botnet.

Peer to peer : Accronyme de l'expression "peer to peer" qui signifie le partage de fichiers (souvent protégés) entre usagers via des sites web tels que thepiratebay.org.

Paquets d'information : Dans le cas des actions par déni de service, l'envoi de paquets d'information fait référence aux requêtes de (re)chargement envoyées depuis un ordinateur vers un site web quelconque.

Script kiddies : Ce terme est utilisé pour faire référence à des militants n'ayant pas de connaissances en programmation informatique. Il s'agit, selon Parmy Olson, de "wannabe hackers" (Olson, 2012, Empl. 1821)

Stuxnet : C'est un virus qui a saboté les usines iraniennes d'énergie nucléaire en 2010. Ce dernier "was designed to disable the centrifuges by inducing rapid fluctuations in the rotation speed of their motors. (...) [O]ne of the most remarkable aspects of the virus was a piece of deception created to confuse Iranians personnel monitoring the plants. Stuxnet secretly recorded what normal operations at the plant looked like, and then played these readings back to the plants operators (...) so that everything seemed to be in good order" (Diebert, 2012, Empl. 2664)

Trolling : Le *trolling* informatique consiste à viser de manière plus ou moins aléatoire des individus ou des groupes d'individus actifs sur l'Internet dans le but de les faire enrager autant que possible (Philipps, 2013b). Ces activités prennent place sur une multitude de plateformes (jeux vidéo en ligne, forums divers, Facebook, Twitter, You Tube, etc.). De plus, les actes de trolling peuvent prendre plusieurs formes, en fonction des groupes menant les opérations et les plateformes, les individus ou les groupes ciblés par les attaques.

Troll : Usagers qui s'adonnent à des activités de trolling.

Wiki : Se dit d'un site web dont le contenu est mis en ligne et modifié par des utilisateurs.

BIBLIOGRAPHIE

A message from Anonymous (2010, 9 décembre) Our Message, Intentions and potential Targets. [Vidéo]. Récupéré de https://www.youtube.com/watch?v=WpwVfl3m32w (Accès le 8 juillet 2014).

Alucar Ex (2011, 5 avril). ANONYMOUS – OPERATION PAYBACK – Sony Press Release. [Vidéo]. Récupéré de https://www.youtube.com/watch?v=2Tm7UKo4IBc (Accès le 8 juillet 2014).

Anonyme (2010a). Operation Avenge Assange. [Image et Texte]. Récupérée de http://knowyourmeme.com/photos/87085-operation-payback (Accès le 8 juillet 2014).

Anonyme (2010b). Operation Payback Limewire. [Image et texte]. Récupéré de https://encyclopediadramatica.es/File:Operationpaybacklimewire.png (Accès le 8 juillet 2014).

Anonyme (2010c). Operation Payback Gallant Macmillan. [Image et texte] Récupéré de https://encyclopediadramatica.es/File:Operation_Payback_GMlegal.png (Accès le 8 juillet 2014).

Anonymous Anarchy (2010, 30 octobre). Operation Payback #Anonymous Message RE :ACTA, SOPA, PIPA, Internet Censorship & Copyright. [Vidéo]. Récupéré de https://www.youtube.com/watch?v=kZNDV4hGUGw (Accès le 8 juillet 2014).

Anonymous6499 (2011, 6 avril). Anonymous : Second press release to Sony. [Vidéo] Récupéré de https://www.youtube.com/watch?v=eryqClObdO8 (Accès le 8 juillet 2014).

Bouldon, J. (2010, 8 décembre). 'Operation Payback' fuels cyberwar. CNN. [Reportage vidéo en ligne] Récupéré de www.cnn.com/video/data/business/2010/12/08/qmb.boulden.operation.payback.cnn.html

Broadhurst, A. R., & Darnell, D. K. (1965). An introduction to cybernetics and information theory.

Bendrath, R. (2003). The American Cyber-Angst and the Real World: Any Link? In R. L. (Ed.) (Ed.), *Bombs and Bandwidth: The Emerging Relationship Between Information Technology ans Security*. New York: New Press.

Cha, A. E. (2010). 4chan users seize Internet's power for mass disruption. *Washington Post, 10 Août 2010*.

Clarke, R. A., & Knake, R. K. (2011). *Cyber war*. New York : HarperCollins, 320p.

CNN Writer Staff (2010, 9 décembre). Pro-WikiLeaks hackers change target to PayPal. CNN. [Article en ligne] Récupéré dehttp://www.cnn.com/2010/WORLD/europe/12/09/world.wikileaks/

Coleman, G. (2009). Net wars over free speech, freedom, and secrecy or how to understand the hacker and Lulz battle against the Church of Scientology. *The Next Hope*(17 mars 2009).

Coleman, G. (2011). Anonymous : From the lulz to collective action. *The News Everyday: A Media Commons Project (6 Avril 2011)*.

Coleman, G. (2012a). Our Weirdness is Free: The Logic of Anonymous - Online Army, Agents of Chaos, and Seeker of Justice. *in. Here Comes Nobody*. https://canopycanopycanopy.com/15/our_weirdness_is_free (Accès 03 décembre 2013) : Triple Canopy.

Coleman, G. (2012 b). Phreaks, Hackers, and Trolls: The Politics of Transgression and Spectacle. In E. b. M. Mandiberg (Ed.), *The Social Media Reader*. New York : New York University Press.

Coleman, G. (2013a). *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton and Oxford: Princeton University Press.

Coleman, G. (2013b). *Anonymous in context: The politics and power behind the mask*. Internet Governance Papers. *Papers No. 3* (September 2013).

Conway, M. (2008). *Media, fear and the hyperreal: the construction of cyberterrorism as the ultimate threat to critical infrastructure* (Vol.

Paper no.2008). Irelande, Dublin City University: Working Papers in International Studies Series. Center for International Studies.

Conway, M. (2009). Le Cyber-Terrorisme : Le discours des médias américains et ses impacts. *Cités, 2009/3*(no39), p.81-94.

Costanza-Chock, S. (2003). Mapping the Repertoire of Electronic Contention. In i. p. Praeger Greenwood (Ed.), *in Andrew Opel and Donnalyn Pompper, eds. Representing Resistance: Media, civil disobedience and the global justice movement*. Wesport.

The Critical Art Ensemble (1996). *Electronic Civil Disobedience and Other Unpopular Ideas*. New York.

CSIS. (2003). Cybercrime, Cyberterrorism, Cyberwarfare. p.15.

Dean, J. (2003). Why the net is not a public sphere. *Constellations*, *10*(1), 95-112.

Dean, J. (2009). *Democracy and other neoliberal fantasies: Communicative capitalism and left politics*. Duke University Press.

De Certeau, M. (1990). *L'Invention du Quotidien*. Paris : Gallimard.

Dennings, D. (2001). Cyberwarriors: Activists and TErrorists Turn to Cyberspace. *Harvard International Review, 23*(2), http://www.hir.harvard.edu/articles/index.html?id=905.

Dominguez, R. (2010). La désobéissance civile électronique : Inventer le Futur du Théâtre d'Agitrop En-Ligne. *Association Multitudes, 2012/2*(#41), p.204-211.

Dwyer, D. (2010, 10 décembre). Foot Soldiers for Wikileaks: 27,000 Download Attack Software Overnight. ABC News. [Article en ligne] Récupéré de http://abcnews.go.com/Technology/wikileaks-anonymous-cyber-attacks/story?id=12355960

Feenberg, A. (2004). *(Re)Penser la technique : Vers une technologie démocratique*. Paris : La Découverte — M.A.U.S.S.

Electrohippies-Collective. (2000). Client-side Distributed Denial-of-Service: Valid Campaign Tactic or Terrorist Act? *Occasional Paper, Vol. 1*.

Foucault, M. (1975). Surveiller et punir : Naissance de la prison. Paris : Gallimard, 360p.

Foucault, M. (1976), « Méthode » in *L'histoire de la Sexualité I. La volonté du savoir,* Paris : Gallimard/Tel, pp. 121-135.

Foucault, M. (1978), « Dialogue sur le pouvoir », in *Dits et écrits*, Tome II, Paris : Gallimard, pp. 464-476.

Foucault, M. (1982). « Le sujet et le pouvoir » in *Dits et écrits*, Tome IV, Paris : Gallimard, pp. 1041-1062.

FOXNEWS (Producer). (2013). Can you protect yourself from cyber-terrorism. http://video.foxnews.com/v/2844292044001/can-you-protect-yourself-from-cyber-terrorism/ — sp=show-clips *(Accès le 25 mars 2014).*

Fox News (2010a, 9 décembre). Cyber-Skirmishes, Street Protests, Rage Over WikiLeaks. Fox News. [Article en ligne] Récupéré de http://www.foxnews.com/tech/2010/12/09/wikileaks-supporters-launch-cyber-attack-amazon/?intcmp=related.

Fox News (2010b, 9 décembre). Facebook, Twitter Delete Pro-WikiLeaks Hackers' Account. Fox News. [Article en ligne] Récupéré de http://www.foxbusiness.com/markets/2010/12/09/facebook-twitter-delete-pro-wikileaks-hackers-account.

Fox News (2010, 9 décembre). Operation Payback Wages War Online. Fox News. [Reportage vidéo en ligne] Récupéré dehttp://video.foxnews.com/v/4453739/operation-payback-wages-war-online/#sp=show-clips.

Fox News (2010, 9 décembre). WikiLeaks 'Data War' Growing, Hacktivists Say. Fox News. [Article en ligne]. Récupéré de http://www.foxnews.com/tech/2010/12/09/wikileaks-data-war-growing-hacktivists-say/?intcmp=related

Fox News Associated Press (2010, 8 décembre). Wikileaks Supporters Launch Cyber Attack on Palin. Fox News. [Article en ligne] Récupéré de http://www.foxnews.com/politics/2010/12/08/sarah-palins-website-attacked-wikileaks-supporters/?intcmp=related

Fox News Associated Press (2013, 3 octobre).Grand jury indicts 13 members of Anonymous. Fox News. [Article en ligne] Récupéré de http://www.foxnews.com/tech/2013/10/03/grand-jury-indicts-13-members-anonymous/

Fox News.com (2010, 8 décembre). Hackers Target WikiLeaks 'Enemies': Mastercard, Twitter, Paypal, Even FoxNews.com. Fox News. [Article en ligne] Récupéré de http://www.foxnews.com/tech/2010/12/08/wikileaks-supporters-launch-hack-attacks/

Francetv.Education (1981). Michel Foucault : le pouvoir comme gouvernementalité. [Vidéo]. Récupéré de http://education.francetv.fr/videos/michel-foucault-le-pouvoir-comme-gouvernementalite-v111212

Fantz, A. et Schubert, A. (2010, 10 décembre). WikiLeaks 'Anonymous' hackers: 'We will fight'. CNN. [Article en ligne] Récupéré de http://www.cnn.com/2010/US/12/09/hackers.wikileaks/

Frieden, T et Candiotti, S. (2011, 20 juillet). 14 hackers arrested in operation targeting Anonymous. CNN. [Article en ligne] Récupéré de http://www.cnn.com/2011/CRIME/07/19/new.york.anonymous.warrants/index.html?iref=allsearch

Freitag, M. (2003). De la terreur au meilleur des mondes. Globalisation et américanisation du monde : vers un totalitarisme systémique? *Presses de l'Université de Laval*, p.359.

Freitag, M. *(2008). L'impasse de la globalisation*. Montréal, Écosociété.

Galloway, A. R. (2004). *How Control Exists After Decentralization*. Cambridge, MA : MIT Press.

Goffman, E. (1974). Frame analysis: An easy on the organization of experience. Cambridge, MA: Harvard University Press

Gordon, S. (2011, 26 juillet). Arlington Home Raided in FBI Hacking Investigation. NBC News. [Article en ligne] Récupéré de http://www.nbcdfw.com/news/tech/Arlington_Home_Raided_in_FBI_Hacking_Investigation_Dallas-Fort_Worth-126157078.html

Gordon, S. (2011, 26 juillet).FBI Raids Arlington House in Hacking Case. NBC News. [Article en ligne] Récupéré de http://www.nbcdfw.com/news/tech/FBI-Raids-Arlington-House-in-Hacking-Case-126151358.html

Greenberg, A. (2012). This Machine Kills Secrets. *New York: Dutton.*

Gross, J.(2011, 27 juillet). Hacker group urges boycott of PayPal. CNN. [Article en ligne] Récupéré de http://www.cnn.com/2011/TECH/web/07/27/anonymous.paypal.message/index.html?iref=allsearch

Hafner, K., & Markoff, J. (1995). *Cyberpunks : Outlaws and Hackers on the Computer Frontier*. New York : Touchstone Simon & Schuster.

Harvey, D. (2005). *A brief history of neoliberalism*. Oxford University Press.

Jäger, S., & Maier, F. (2009). Theoretical and methodological aspects of Foucauldian critical discourse analysis and dispositive analysis. *Methods of critical discourse analysis*, *2*, 34-61.

Housh, G. (2011, 10 août). Gregg Housh explains the ideology of the group 'Anonymous'. CNN. [Reportage vidéo en ligne] Récupéré de http://www.cnn.com/2010/US/12/09/hackers.wikileaks/

Jenkins, J. (2010). Man trolled the Web for girls : cops; Police seek possible victims after undercover sting. *Toronto Sun*(7 décembre 2010), HTTP://cnews.canoe.ca/CNEWS/Crime/2007/2012/2007/4712680-sun.html

Jordan, T. (2008). *Hacking : Digital Media and Technological Determinism*. Cambridge : Polity Press.

Jordan, T., & Taylor, P. (2004). *Hacktivism and Cyberwars: Rebels with a Cause?* London and New York : Routledge Taylor and Francis Group.

Kaplan, J. (2010, 9 décembre). We Want YOU, Say Hacktivists ... but Is It Legal? Fox News. [Article en ligne] Récupéré de http://www.foxnews.com/tech/2010/12/09/wikileaks-operation-payback-hacktivists-legal/

Knight, W. (2009). License to hack? — Ethical Hacking. http://www.infosecurity-magazine.com/view/4611/license-to-hack-ethical-hacking / *(Accès le 28 mars 2014).*

KNOW YOUR MEME, Operation Payback. http://knowyourmeme.com/memes/events/operation-payback (Page consultée le 10 mai 2014).

Knutilla, L. (2011). User unknown: 4chan, anonymity and contigency. *First Monday: Peer-Reviewed Journal on the Internet*. http://firstmonday.org/ojs/index.php/fm/article/view/3665/3055 *(Accès le 10 mars 2014)*.

Lafontaine, C. (2004). L'empire cybernétique. Des machines à penser à la pensée machine. *Éditions du Seuil, Paris*.

Lessig, L. (2006). Code And Other Laws of Cyberpace, Version 2.0.

Lessig, L. (2003). Dunwody Distinguished Lecture in Law: The Creative Commons. *Florida Law Review, 55*(3), p.763-777.

Levy, S. (1985). *Hackers : Heroes of the Computer Revolution*: O'Reilly Media, Inc.

Liang, L. (2010). Beyond Representation: The Figure of the Pirate *Access to Knowledge in the Age of Intellectual Property* (pp. p.353-375). New York : Zone Books.

Linebaugh, P., & Rediker, M. (2002). *The Many-Headed Hydra: Sailor, Slave, Commoners, and the Hidden History of the Revolutionary Atlantic*. Boston: Beacon Press.

Luckerhoff, J. Approches inductives. (En ligne) https://oraprdnt.uqtr.uquebec.ca/pls/public/gscw031?owa_no_site=1707&owa_no_fiche=67. (Page consultée le 15 mai 2014).

MacFarland, KT et Hunt R. (2010, 9 décembre). Wiki-War: Operation Payback. [Article en ligne] Récupéré de http://video.foxnews.com/v/4454282/wiki-war-operation-payback/#sp=show-clips

MacLeod, A., Dufault, E., Dufour, F. G., & Morin, D. (2008). *Relations internationales, théories et concepts*. Montréal: Athéna Éditions.

McDermott, Q. (2012, 17 juillet). 'Operation Payback' accused says he has no regrets. ABC News. [Article en ligne] Récupéré de http://www.abc.net.au/news/2012-06-18/anonymous-four-corners/4077476

Marcuse, H. (1968). *L'Homme unidimensionnel : Essai sur l'idéologie de la société industrielle avancée*. Paris : Éditions Minuit.

Mattelart, A. (2010). Gouverner par la trace. *La Découverte/Mouvements, 2010/2*(62), p.11-21.

Mattelart, A. (2007). *La globalisation de la surveillance*. Paris : La Découverte.

Mondoux, A. (2011a). *Histoire sociale des technologies numériques de 1945 à nos jours*. Montréal : Éditions Nota Bene.

Mondoux, A. (2011 b). Identité numérique et surveillance. *Les cahiers du numérique, Vol.7*(2011/1), p.49-59.

Mondoux, A. (2012). Technique et individuation: la part du social. *Mobilisation de l'objet technique dans la production de soi, Presses de l'Université du Québec, collection Cahiers du Gerse*, 37-56.

Moore, A. (2006). *V for Vendetta*. Gramedia Pustaka Utama.

Mouffe, C. (2005). *On the political*. Taylor & Francis.

National-Research-Council. (1991). *Computers at Risk: Safe Computing in the Information Age*. Washington, DC: National Academy Press: https://http://www.nap.edu/books/0309043883/html/index.html (Accès le 18 mars 2014).

Nelson, B., Choi, R., Iacobucci, M., & Gagnon, G. (1999). Cyberterror: Prospects and Implications. *Center for the Study of Terrorism and Irrefular Warfare*, http://www.nps.navy.mil/ctiw/files/Cyberterror Prospects and Implications.pdf *(Accès 18 mars 2014)*.

Nightly News MSNBC.com (2011, 9 mars). Inside CyberWars. MSNBC. [Reportage Vidéo en ligne] Récupéré de https://www.youtube.com/watch?v=ueoxXAuFTsM

Non précisé (2011, 7 janvier). The Top Four Cyber Threats for 2011. ABC News. [Article en ligne] Récupéré de http://abcnews.go.com/Blotter/cyber-threats-2011-age-stuxnet-hacktivists-social-spammers/story?id=12555830

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

Olderman, K. (2010, 10 décembre). News on Anonymous Operation Payback. MSNBC. [Reportage vidéo en ligne] Récupéré de https://www.youtube.com/watch?v=ye_F0w5nP5w

Olson, P. (2012). *We are Anonymous: inside the hacker world of Lulzsec, Anonymous, and the global cyber insurgency*. Hachette Digital, Inc.

Operation Payback (2010, 29 octobre). What is Operation : Payback ?. [Vidéo]. Récupéré de https://www.youtube.com/watch?v=Vp-wXWGRM18 (Accès le 4 juillet 2014).

Pew Research Center (2014), « Cable TV Viewership ». [En ligne] http://www.journalism.org/2014/03/26/state-of-the-news-media-2014-key-indicators-in-media-and-news/1-cable-tv-viewership/ (Accès le 01 juin 2014)

Pew Research Center (2013), « Evening News Viewership by Network ». [En ligne] http://www.journalism.org/media-indicators/evening-news-viewership-by-network/ (Accès le 01 juin 2014).

Pham, S. (2010, 8 décembre). Exclusive: Sarah Palin Under Cyber-Attack from Wikileaks Supporters in "Operation Payback". ABCNews. [Article en ligne] Récupéré de http://abcnews.go.com/blogs/politics/2010/12/exclusive-palin-under-cyber-attack-from-wikileaks-supporters-in-operation-payback/

Phillips, W. (2013a). The House That Fox Built: Anonymous, Spectacle, and Cycles of Amplification. *Television & New Media, Novembre 2013*(14), p. 494-509.

Phillips, W. (2013 b). LOLing at tragedy: Facebook trolls, memorial pages and resistance to grief online. *First Monday : Peer-review Journal on the Internet,* http://firstmonday.org/ojs/index.php/fm/article/view/3168/3115 *(Accès le 21 février 2013).*

Rainbow, P., & Rose, N. (2003). The essential Foucault. New York: the New Press.

Rasch, M et Todd, M. (2010, 8 décembre). CNN's Briand Todd investigates claims that Visa and MasterCard are under cyber attack from supporters of Julian Assange. CNN. [Reportage vidéo en ligne] Récupéré de www.cnn.com/2010/US/12/09/hackers.wikileaks

Ryan, J. (2011, 13 décembre). FBI Arrests 'Anonymous' Member for Attack Against GeneSimmons.com. ABC News.[Article en ligne] Récupéré de http://abcnews.go.com/blogs/politics/2011/12/fbi-arrests-anonymous-member-for-attack-against-genesimmons-com/

Ryan, J. (2011, 27 janvier). Wikileaks Cyberattacks : FBI Executes More Than 40 Search Warrants Across US. ABC News. Récupéré de http://abcnews.go.com/International/wikileaks-cyberattacks-fbi-executes-40-search-warrants-us/story?id=12782171

Resweber, J-P. (2004), « L'écriture de l'histoire », *Le Portique* [En ligne], 13-14 | 2004, mis en ligne le 15 juin 2007, consulté le 08 juillet 2014. URL : http://leportique.revues.org/637

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

Sauter, M. (2013). "LOIC Will Tear Us Apart": The Impact of Tool Design and Media Portrayals in the Success of Activist DDOS Attacks. *American Behavioral Scientist, 57*(7), p.983-1007.

Söderberg, J. (2013). Determining social change: The role of technological determinism in the collective framing of hackers. *New Media and Society, Vol. 1*(Issue. 17).

Schubert, A. (2010, 8 décembre). Hacker 'activists' target Mastercard. CNN. [Reportage vidéo en ligne] Récupéré de http://www.cnn.com/2010/US/12/09/hackers.wikileaks/

Schuetter, J. (2011, 9 décembre). How far will Wikileaks Cyber war go?. CNN. [Reportage vidéo en ligne] Récupéré de http://www.cnn.com/2010/WORLD/europe/12/09/world.wikileaks/

Sciutto, J. (2010) Wikileaks Crackdown Prompts Cyber Attacks. ABC News. [Reportage vidéo en ligne] Récupéré de http://abcnews.go.com/International/wikileaks-cyberattacks-fbi-executes-40-search-warrants-us/story?id=12782171

Sciutto, J., Ferran, Lee et Goldman, R. (2010, 9 décembre). Lawyer: Assange Accusers 'Treated Like Perpetrators'. ABC News. [Article en ligne] Récupéré

de http://abcnews.go.com/US/operation-payback-anonymous-cyber-battle-erupts-wikileaks/story?id=12351428&page=2

Shuetter, J.(2010, 10 décembre). Explain it to me: Cyber attacks. CNN. [Reportage vidéo en ligne]Récupéré de www.cnn.com/2010/US/12/09/hacker.wikileaks

Smith, A. (2010, 8 décembre). MasterCard, Visa targeted in apparent cyberattack.CNN. [Article en ligne] Récupéré de http://money.cnn.com/2010/12/08/news/companies/mastercard_wiki/

Stark, L. et Muir, D (2012, 2 mai). Anonymous Hacker's High Profile Targets. ABC News. [Reportage vidéo en ligne]. Récupéré de http://abcnews.go.com/WNT/video/anonymous-hackers-high-profile-targets-governments-businesses-cyber-threat-technology-15518717

Sterling, B. (1992). The hacker crackdown: Law and Disorder on the Electronic Frontier. 1992. *Bantam, New York.*

Sy, S. (2011, 20 juillet). Hackers Arrest: More than a Dozen Suspects. ABC News. [Article en ligne] Récupéré de http://abcnews.go.com/WNT/video/abc-news-update-14118047

Tarrow, S. (1994). *Power in Movement : Social Movements and Contentious Politics*. Cambridge : Cambridge University Press.

Tilly, C., & Tarrow, S. (2007). *Contentious Politics*. Boulder, CO : Paradigm Publishers.

TheHairyHeart (2010, 11 décembre). ANON OPS : A Press Release : December 10, 2010. [Vidéo]. Récupéré de https://www.youtube.com/watch?v=fxT3Bn7_-Ig (Accès le 8 juillet 2014).

V for Vendetta. Warner Home Video, 2012.

Wiener, N. (1965). *Cybernetics or Control and Communication in the Animal and the Machine* (Vol. 25). MIT press.

Wolfe, B. (2011, 19 juillet). Anonymous hackers Arrested by FBI. ABC News.[Article en ligne] Récupéré de http://abcnews.go.com/blogs/politics/2011/07/anonymous-hakcers-arrested-by-fbi-wikileaks-operation-payback-assange

Young, R., Zhang, L., & Prybutok, V. R. (2007). Hacking into the Minds of Hackers. *Information Sustems Management, 24*(4).

Žižek, S. (2002). *Welcome to the desert of the real!: five essays on September 11 and related dates*. Verso.