Criminologie, Forensique et Sécurité

www.revue-cfs.net | ISSN : 2813-6098

Organe officiel de l'association internationale des criminologues de langue française (AICLF)

Article régulier

Criminologie, Forensique et Sécurité

2025 | 3 (1) : 3993

https://doi.org/10.26034/la.cfs.2025.3993

Opération Québec : L'utilisation de la théorie de l'association différentielle pour comprendre le processus d'apprentissage du piratage chez les membres d'Anonymous

Francesco C. Campisi[1] **et Francis Fortin**[1]

[1]L'École de criminologie, Université de Montréal, Montréal, QC, Canada

Contact : francesco.carlo.campisi@umontreal.ca

Résumé

Depuis 2008, *Anonymous*, un groupe hacktiviste décentralisé et inclusif, a lancé des centaines de campagnes singulières, éphémères et similaires, ciblant principalement les infrastructures en ligne des gouvernements et privilégiant certains types de cyberattaques (Coleman, 2020 ; Steinmetz, 2022). En raison de la normalisation de la sélection des cibles et des cyberattaques, nous avons utilisé la théorie de l'association différentielle pour comprendre si l'association entre pairs facilite le processus d'apprentissage des nouveaux membres d'Anonymous (appelé « Anons ») au cours d'une campagne de piratage. Les données proviennent de conversations sur des forums IRC (« internet relay chats ») durant le Printemps Érable de 2012 au Québec, où Anonymous a piraté différents sites web gouvernementaux. Les résultats indiquent que les techniques de piratage constantes sont dues à l'utilisation de ressources d'apprentissage préétablies, qui assurent l'apprentissage de techniques et de motivations similaires. Les pairs dans ces forums encourageant les nouveaux Anons à pirater le gouvernement en associant une moralité à certaines cibles jugées légitimes et à affiner leurs compétences individuelles, tout en inculquant des valeurs normatives définissant les cibles légitimes et illégitimes. Ces novices sont encouragés à renforcer leur approbation de ces comportements en promouvant les actes d'Anonymous sur les médias sociaux. Cet environnement en ligne peut transformer des novices en pirates compétents, augmentant le potentiel de futures campagnes.

Mots clés

Cybercriminalité, désobéissance numérique, apprentissage en ligne, communautés virtuelles, sous-cultures hacktivistes

Operation Quebec: Using Differential Association Theory to Understand the Hacking Learning Process Among Anonymous Members

Abstract

Since 2008, the decentralized and inclusive hacktivist group *Anonymous* has launched hundreds of stand-alone campaigns, primarily targeting government using certain hacking techniques (Coleman, 2020; Steinmetz, 2022). Due to the standardization of both target selection and types of cyberattacks, we used Differential Association theory to understand whether peer association facilitates the learning process of new Anonymous members (known as "Anons") during a hacking campaign. The data derives from IRC conversations during the 2012 Maple Spring Protests, where Anons hacked the Québec provincial government. A thematic content analysis suggests that Anonymous' consistency stems from the use of pre-established resources that ensure all participants learn similar techniques and motivations that can be applied across all campaigns. Congruent with the tenents of Differential Association theory, our results indicate that peers in the chats sustained the learning process of newcomers, not only transmitting technical skills but also inculcating values and definitions that distinguish legitimate from illegitimate targets. Newcomers are also encouraged to reinforce their approval of such behaviors by promoting Anonymous' hacks on social media. Together, this online environment can transform novices into proficient hackers, increasing the potential for future campaigns.

Keywords

Cybercrime, digital disobedience, online activism, virtual communities, hacktivist subcultures

Citation : Francesco C. Campisi, Francis Fortin. (2025) Opération Québec : L'utilisation de la théorie de l'association différentielle pour comprendre le processus d'apprentissage du piratage chez les membres d'Anonymous. *Criminologie, Forensique et Sécurité*, 3 (1) : 3993.

Introduction

En 2012, la plus longue grève étudiante de l'histoire du Canada a eu lieu au Québec. Appelée « Printemps Érable » (un hommage au « printemps arabe »), elle faisait suite à une proposition du gouvernement provincial d'augmenter les frais de scolarité de 75 % dans les universités québécoises (Bégin-Caouette et Jones, 2014 ; CBC News, 2012). Après des mois de protestations, le projet de loi 78 qui restreignait la liberté d'association des individus et accordait plus de pouvoirs aux policiers a été proposé, provoquant des affrontements violents avec des émeutiers (Léger, 2019 ; Levesque, 2012 ; Raynauld *et al.*, 2016). La loi éphémère 78 a déclenché l'Opération Québec, une opération de piratage informatique menée par le groupe « Anonymous » qui a visé les sites web gouvernementaux en réponse à la restriction de la liberté de manifester (Levesque, 2012). Entre les mois d'avril et de mai 2012, les Anons ont piraté et ont temporairement mis hors service plusieurs sites web gouvernementaux, dont celui du ministre québécois de la Sécurité publique, le site web du parti libéral du Québec (le gouvernement au pouvoir), le site web de l'aide financière aux études du Québec, le site web du ministre de l'éducation, du loisir et du sport du Québec, le site web de l'assemblée nationale du Québec et celui du commissaire à la déontologie policière (Daudens, 2012).

La plupart des techniques de piratage nécessitent un certain niveau de connaissances techniques et font, par conséquent, l'objet d'un processus d'apprentissage complexe. La théorie de l'association différentielle postule que tous les comportements, y compris les actes criminels, tels que le piratage, sont appris par association avec un groupe de pairs (Sutherland *et al.*, 1992). Elle suggère que les individus acquièrent les compétences, les motivations et les attitudes nécessaires pour commettre des actes déviants en s'associant à des pairs délinquants. Des études récentes sur les communautés de pirates informatiques confirment la validité de cette théorie et mettent en évidence l'aide mutuelle au sein de leurs pairs virtuels, favorisés par le partage d'informations et transmettre les outils nécessaires pour apprendre à pirater (Décary-Hétu, 2014 ; Levin *et al.*, 2012 ; Morris, 2011 ; Morris et Blackburn, 2009).

Cependant, les processus d'apprentissage chez les Anons diffèrent de ceux des pirates traditionnels. D'abord, la motivation est différente ; Anonymous n'est pas motivé par le profit économique, mais par le désir de changer l'opinion publique (Li, 2013), ce qui leur vaut la qualification de groupe hacktiviste. Ensuite, les communautés de pirates ont tendance à éviter la visibilité publique au cours de leurs opérations de piratage informatique (Décary-Hétu, 2014). En revanche, Anonymous se démarque par ses cyberattaques publiques, médiatisées via les réseaux sociaux (Beraldo, 2022 ; Jones *et al.*, 2020, 2022).

La capacité d'Anonymous à transférer des compétences techniques, attitudes et motivations, selon la théorie de l'association différentielle, demeure largement méconnue. Les études antérieures se sont concentrées sur l'histoire du collectif hacktiviste (Bardeau et Danet, 2011 ; Dobusch et Schoeneborn, 2015 ; Guiton, 2013 ; Jul, 2013 ; Klein, 2015) ou sur ses activités en ligne (Bergeron *et al.*, 2019 ; Machado, 2015 ; Mansfield-Devine, 2011 ; McGovern et Fortin, 2019), ou une combinaison des deux (Coleman, 2014 ; Olsen, 2012), négligeant ainsi le processus d'apprentissage des comportements et le transfert de compétences techniques. Malgré sa structure nébuleuse et informelle, où les campagnes sont lancées indépendamment avec des compétences techniques variées (Caldwell, 2015 ; Jul, 2013 ; Kelly, 2012), Anonymous a la réputation d'utiliser certaines techniques de piratage, en particulier les attaques par déni de service distribuées (DDoS) et la défiguration de sites web contre des cibles gouvernementales (de la Hamaide, 2015 ; Fortin *et al.*, 2022 ; Purtill, 2022), qui caractérisent le groupe depuis plus d'une douzaine d'années.

À ce titre, cette étude mobilise le cadre de la théorie de l'association différentielle pour mieux comprendre le processus d'apprentissage des membres d'Anonymous d'un réseau de hacktivistes par ailleurs décentralisé. Nous analysons les activités de la cellule québécoise d'Anonymous dans deux forums IRC publics durant les manifestations du Printemps Érable, où ils ont discuté, planifié, exécuté et organisé leurs cyberattaques contre le gouvernement du Québec. Ainsi, cela offre l'opportunité d'examiner si ces forums favorisent une communauté propice à l'apprentissage de nouveaux comportements, ainsi que des exemples concrets de partage de compétences techniques, de motivations et d'attitudes qui augmentent la volonté de participer à de telles actions. Étant caractérisées par leur réactivité, leur spontanéité et leur imprévisibilité (voir Coleman, 2020), les données issues des forums IRC sont rares et offrent une opportunité d'analyser comment les compétences techniques, motivations et attitudes sont développées, utilisées et partagées dans une opération de piratage.

La revue de littérature

L'association différentielle et le piratage informatique

S'ajoutant à la littérature existante sur les théories de l'apprentissage social, Sutherland a proposé une théorie selon laquelle le comportement criminel est appris par le biais d'un processus dynamique continu d'interactions entre pairs délinquants (Sutherland *et al.*, 1992). La théorie de l'association différentielle part du principe que tout comportement s'apprend lorsqu'un individu intériorise des techniques, des motivations et des attitudes favorables à l'acte. La théorie fait porter la responsabilité des comportements acquis sur l'association avec les pairs, en soutenant que les pairs antisociaux peuvent conduire à des comportements antisociaux. Jusqu'à présent, plusieurs études ont utilisé cette théorie pour expliquer l'apprentissage des comportements de groupes informels décentralisés, tels que les gangs de rue de jeunes (Gagnon, 2018) ainsi que d'autres communautés de piratage numérique (Décary-Hétu, 2014 ; Levin *et al.*, 2012 ; Morris et Higgins, 2010).

Ainsi, Sutherland *et al.* (1992) propose neuf principes de l'apprentissage d'un comportement criminel qui se distinguent par trois affirmations latentes : la première affirmation soutient que l'association de pairs délinquants peut entrainer un comportement délinquant individuel.

Cette affirmation suggère que l'apprentissage de tout type de comportement découle d'un processus interactif, où la présence d'un comportement parmi les pairs peut mettre en œuvre le processus d'apprentissage des autres membres. Par exemple, les recherches sur le piratage informatique ont mis en évidence l'existence d'une communauté virtuelle d'intime de pairs qui offre à ses membres un soutien et une reconnaissance par ces pairs (Décary-Hétu, 2014 ; Morris et Blackburn, 2009). D'autres études indiquent que des relations formelles ne sont pas nécessaires pour l'apprentissage des comportements criminels en ligne, mais que la simple exposition à un comportement délinquant peut faciliter ce processus (Marcum *et al.*, 2014 ; Warr et Stafford, 1991). En comparaison avec les affirmations de Décary-Hétu (2014) et Morris et Blackburn (2009), ces études suggèrent que n'importe qui dans la communauté peut aider un individu, avec de multiples relations informelles et collaboratives qui guident l'individu.

La deuxième affirmation indique que le processus d'apprentissage est complémenté par des pairs expérimentés qui transmettent les ressources spécifiques nécessaires à l'apprentissage des comportements. Par exemple, dans le cas d'une communauté de pirates informatiques s'engageant dans une escroquerie par hameçonnage du courrier électronique de PayPal, le kit (un code préconstruit pour un type spécifique de piratage) a été transmis par le biais de communications virtuelles dans des forums spécifiques pour ceux qui étaient prêts à l'utiliser (Levin *et al.*, 2012). Au sein des communautés de pirates informatiques criminels, les compétences technologiques sont principalement échangées, avec des pirates moins expérimentés recherchant des conseils auprès des plus expérimentés en renforçant l'indépendance individuelle et fournissant les ressources nécessaires au développement des compétences techniques (Babko-Malaya *et al.*, 2017 ; Morselli *et al.*, 2006). Levin *et al.* (2012) affirment que des pirates agissaient comme professeurs du crime sur ces forums.

La troisième affirmation soutient que les groupes de pairs délinquants peuvent également transmettre les cognitions, les motivations, les rationalisations et les attitudes (classées ici sous le terme « définitions ») nécessaires pour intérioriser la volonté de commettre des actes criminels (Décary-Hétu, 2014 ; Sutherland *et al.*, 1992). Lorsqu'un individu intériorise des définitions qui favorisent grandement les comportements criminels, il est plus susceptible de s'engager dans de tels comportements. Les communautés de pirates transmettent des attitudes concernant les normes sociales au sein de la communauté et un langage commun pour renforcer l'adhésion des pairs (Morris et Blackburn, 2009). Par exemple, par la transmission des attitudes et des motivations qui valorisent le gain monétaire à tout prix, ou en créditant d'autres personnes ayant déjà utilisé les kits sans répercussions comme justifications favorables pour commettre une fraude en ligne (Levin *et al.*, 2012). Ces définitions diffusées à travers leur réseau de pairs normalisent l'utilisation des techniques d'hameçonnage et neutralisent les sentiments de culpabilité chez les participants hésitants, aidant ainsi les nouveaux pirates à s'identifier à la communauté des pirates et à accepter leurs normes déviantes et rationalisations favorables aux comportements déviants.

Anonymous et le piratage informatique

À la différence des pirates informatiques, les « hacktivistes » utilisent des technologies numériques pour perturber et pour remettre en question les systèmes et protocoles établis qui ont traditionnellement défini les institutions de pouvoir (Gunkel, 2005 ; Renzi, 2015). Anonymous, par exemple, idéalise et défend le partage de l'information, en ciblant les institutions et acteurs qui portent atteinte aux droits, tels que la liberté d'expression et la liberté d'information (Bodó, 2014 ; Coleman, 2020 ; Fortin *et al.*, 2022 ; Kenney, 2015). Les résultats potentiels de ces campagnes peuvent inclure des dommages en volant des documents exclusifs, en fermant des sites web et des services, et, lorsqu'ils sont ciblés, peuvent entrainer des pertes financières pour les banques (George et Leidner, 2019 ; Schrock, 2016 ; Steinmetz, 2022).

Des années de recherche sur les opérations d'Anonymous révèlent un schéma selon lequel les membres d'Anonymous préfèrent un petit nombre de techniques de piratage contre les institutions du pouvoir : les attaques par déni de service distribuées (DDoS), la défiguration de sites web et le doxing. Les attaques par déni de service distribué (DDoS), où ils tentent de mettre hors service les sites web d'organisations cibles en les inondant de requêtes simultanées, constituent la cyberattaque la plus courante dans l'arsenal d'Anonymous, car elles nécessitent très peu de compétences par rapport à la défiguration de sites web qui exige une certaine connaissance du codage (Bodó, 2014). Durant l'opération Québec, les participants de la campagne de piratage ont principalement utilisé des attaques DDoS, bien que les attaques contre l'Assemblée nationale du Québec soient considérées comme une défiguration de site web, car la phrase « On a honte de notre gouvernement » a été affichée sur la première page du site web avant d'être supprimée plus tard ce jour-là (Daudens, 2012). Le doxing (défini comme la révélation d'informations hautement privées sur une cible) est aussi complexe techniquement que la défiguration d'un site web et, bien qu'elle ait été utilisée dans plusieurs autres campagnes de piratage (par exemple, #OpérationMinneapolis), il n'existe aucune preuve de l'utilisation du doxing au cours de l'opération Québec (Molloy et Tidy, 2020).

Par ailleurs, la structure organisationnelle d'Anonymous se caractérise généralement par une forme nébuleuse et imprécise, avec de petits groupes structurés horizontalement plutôt que par une hiérarchie formelle (Machado, 2015 ; Mansfield-Devine, 2011). Après l'arrestation de certains de ses dirigeants en 2012, la dissolution de ses branches militantes (AntiSec et LulSec) et le suicide du célèbre Anon Aaron Swartz, le groupe est devenu encore plus décentralisé, avec des campagnes autonomes lancées indépendamment (Anderson, 2012 ; Coleman, 2020 ; Kelly, 2012). De plus, Fortin *et al.* (2022) ont noté qu'Anonymous attache une importance particulière à la liberté d'information et à la liberté d'expression, ce qui a conduit à la création de nombreuses campagnes singulières, abordant diverses questions sociopolitiques, telles que l'environnement, les abus de pouvoir et l'hypersurveillance (Jul, 2013; Klein, 2015 ; McGovern et Fortin, 2019).

Problématique et objectif de l'étude

L'absence de forme et de structure définies dans les interactions entre les membres d'Anonymous rend la compréhension de la dynamique entre eux difficile pour les chercheurs sur les mouvements sociaux. Contrairement à d'autres communautés de pirates, où des formes d'aide formelles et informelles peuvent être identifiées, Anonymous ne suit pas de systèmes organisationnels clairement définis. Malgré cela, les campagnes fructueuses de piratage menées par Anonymous montrent qu'ils maîtrisent des techniques, suggérant qu'un certain type d'apprentissage et de partage d'informations doit avoir lieu au sein du groupe. Malgré cette hypothèse, la capacité d'Anonymous à transférer des compétences techniques et des définitions, comme le suggère la théorie de l'association différentielle, reste largement méconnue, et les informations sur l'apprentissage des comportements au sein du groupe sont vagues, sans discussion supplémentaire sur le transfert de compétences techniques. Cela nous oblige à poser la question : comment les recrues d'Anonymous acquièrent-elles ces compétences techniques nécessaires pour pirater de manière uniforme ?

La présente étude vise à démystifier les interactions au cours d'une opération de piratage d'Anonymous, afin de comprendre si l'association de pairs en ligne est propice à un processus d'apprentissage normalisé pour les nouveaux Anons. Ainsi, une analyse des échanges entre les membres des forums (appelés Internet Relay Chat [IRC] durant l'Opération « Québec ») est effectuée pour identifier la présence de trois affirmations : (1) l'existence d'une communauté virtuelle qui encourage les relations entre pairs bénéfiques pour l'apprentissage de la délinquance ; (2) l'apprentissage des compétences techniques requises auprès des autres membres, que ce soit par le biais d'une association et d'une collaboration informelle entre pairs, ou par le biais d'une structure d'apprentissage hiérarchique plus formelle ; (3) l'apprentissage des définitions qui favorisent l'engagement dans une campagne de piratage (c'est-à-dire les motivations, les attitudes et les valeurs) qui est favorable à l'utilisation des techniques de piratage contre leur cible.

Méthodologie

Données

La base de données pour la recherche actuelle a été obtenue à partir de deux forums accessibles au public et utilisés par les membres d'Anonymous pendant leur campagne de piratage qui a duré environ deux mois au printemps 2012. Bien que la présence d'Anonymous sur les réseaux sociaux soit indéniable, ces plateformes sont principalement utilisées pour mettre en valeur leurs cyberattaques et discuter de questions à portée politique ou sociale, plutôt que pour organiser directement des opérations, compte tenu de leur caractère public et facilement surveillable (Fortin *et al.*, 2022). Les forums IRC sont des forums publics ou privés qui permettent aux utilisateurs d'échanger entre eux, la plateforme offrant la possibilité d'une communication en temps réel, même si, dans la pratique certains échanges peuvent aussi se dérouler de manière asynchrone. Leur principale caractéristique est la possibilité pour les utilisateurs de rester anonymes, grâce à des proxys qui dissimulent l'adresse IP des utilisateurs (Décary-Hétu et Leppänen, 2013). Ainsi, le choix de se concentrer sur les IRC s'explique par le fait qu'ils permettent d'observer des communications plus étroitement liées à la préparation des cyberattaques et aux interactions entourant ces actes.

La source principale des données est constituée des fichiers journaux « *logs* » des chambres publiques d'Anonymous fournis par la Sûreté du Québec (SQ) en 2012 dans le cadre de l'enquête sur l'opération Québec. Ces fichiers contenaient, pour chaque message, des métadonnées incluant l'horodatage et le pseudonyme de l'utilisateur. Le corpus de données relatives au collectif Anonymous, réparti entre deux chambres de discussion, comprend 447 fichiers totalisant environ 21 mégaoctets de données et 259 668 lignes de texte.

Il n'a pas été nécessaire de procéder à une anonymisation supplémentaire des adresses IP, puisque les chambres IRC les masquent déjà grâce à l'utilisation de proxys. Toutefois, afin de protéger davantage les participants, tous les pseudonymes présents dans les *logs* ont été remplacés par des identifiants anonymes uniques et cohérents, de sorte qu'un même pseudonyme soit toujours associé au même identifiant tout au long du corpus. Par ailleurs, les extraits reproduits dans l'article ne comportent ni la date précise des échanges ni l'identifiant des chambres IRC, et les pseudonymes anonymisés ne sont pas liés aux adresses IP réelles. Même en recoupant ces informations, il serait donc impossible d'identifier un auteur. Sur le plan éthique, nous avons retenu trois principes : (1) l'analyse s'est limitée à des espaces publics déjà accessibles et non protégés par un mot de passe, (2) les données utilisées nous ont été fournies par une autorité policière dans le cadre légal d'une enquête et (3) les identifiants personnels ou adresses IP n'étaient pas disponibles dans les fichiers. De ce fait, le risque d'identification individuelle est minimal, et l'analyse a été conduite conformément aux principes éthiques de recherche portant sur les données publiques en ligne.

Stratégie analytique

Les fichiers ont été vérifiés afin d'en assurer l'intégrité, les messages système (notifications de connexion/déconnexion) supprimés, et les pseudonymes ont été remplacés par des identifiants anonymes uniques et cohérents (tout en uniformisant la casse et en supprimant les suffixes techniques ajoutés automatiquement par la plateforme), puis l'ensemble a été converti en format texte standard avant d'être importé dans QDA Miner (version 4.0) pour le codage. QDA Miner est un logiciel d'analyse de données utilisé pour coder, thématiser et segmenter les textes (Géring, 2021). Ce logiciel est privilégié pour analyser les textes issus des plateformes en ligne, qui sont souvent structurés comme des ensembles de données étendues et des conversations fragmentées, où il y a peu de linéarité dans le processus conversationnel (Chen et Wang, 2019). Dans le cadre de cette étude, le logiciel a été utilisé comme outil d'assistance à l'analyse manuelle, et non comme un dispositif de traitement automatique du langage naturel. L'attribution des thèmes ne s'est donc pas faite par appariement d'expressions régulières, par « clusterisation » ni par pondération TF-IDF, mais par un processus de codage manuel systématique effectué par les chercheurs. Concrètement, chaque message a été lu individuellement (analyse verticale) et codé selon son sujet. Un message pouvait être associé à plusieurs thèmes lorsqu'il comportait différentes dimensions.

Ce premier cycle de codage a permis de créer des thèmes spécifiques liés, par exemple, aux croyances, aux motivations ou encore à certains évènements et différends. L'intérêt de cette approche est qu'elle offre un avantage considérable en permettant aux chercheurs de s'immerger dans le contexte de l'époque : l'analyse quotidienne des échanges a révélé les valeurs, le mode de vie, la personnalité et les motivations d'adhésion des participants, fournissant des informations uniques et difficilement accessibles par d'autres méthodes, comme un sondage.

Dans un second temps, les thèmes ont été regroupés en catégories plus larges caractérisant les discussions, puis organisés en fonction des objectifs de recherche. Six dimensions principales ont émergé : (1) l'identification collective, (2) les valeurs associées à la liberté de l'information, (3) les valeurs relatives aux médias traditionnels, (4) le processus de sélection des cibles, (5) les techniques de piratage employées et (6) les perceptions et réactions après les opérations. Ce processus a permis de construire une description riche et nuancée des interactions, en particulier pour observer si l'apprentissage des nouveaux membres correspond aux mécanismes postulés par la théorie de l'association différentielle. Par exemple, l'extrait suivant a été codé dans le thème des « techniques de piratage employées », et sous-codifié en « apprentissage par les autres » :

> [01:10] <ExempleUsager1> que signifie BOOSTER ?
> [01:11] <ExempleUsage2> un booster est un script que hoic utilise pour augmenter l'efficacité de l'attaque et aider à empêcher l'attaque d'être atténuée

Cet échange illustre un moment d'apprentissage entre pairs où un membre plus expérimenté transmet une connaissance technique à un nouvel arrivant.

Résultats

Sur le plan thématique, les deux chambres ont donné lieu à des conversations très différentes. Le premier regroupait une multitude de discussions sur les valeurs d'Anonymous et leur approche préférée pour la sélection des cibles et l'organisation des attaques. Dans la seconde, les discussions portaient principalement sur les évènements qui se sont déroulés pendant le Printemps Érable au Québec. Ces deux espaces ont également permis d'identifier des échanges de compétences techniques entre pairs, révélant la manière dont les connaissances circulaient au sein du collectif. D'un point de vue empirique, le corpus analysé compte 259 668 lignes de textes, mais ce volume important ne doit pas masquer le fait qu'il provient principalement d'un petit noyau d'usagers. Les soixante utilisateurs les plus actifs ont produit en moyenne 1 011 messages, mais cette moyenne masque une forte disparité : une minorité d'individus était particulièrement prolifique, alors qu'une majorité d'usagers ne participait que de façon occasionnelle, parfois en n'envoyant qu'un seul message

Afin d'illustrer les dynamiques dégagées par cette analyse, nous présentons ci-dessous une série d'extraits significatifs. Ces extraits doivent être compris comme des illustrations qualitatives de tendances récurrentes observées dans le corpus, et non comme une mesure statistique de leur fréquence. Nous reconnaissons que des comptages systématiques auraient permis d'apporter un éclairage complémentaire sur l'ampleur relative de certains phénomènes, mais l'objectif de cette étude est de mettre en évidence les mécanismes sociaux et les logiques d'apprentissage entre pairs. Dans ce cadre, la force des extraits repose sur leur capacité à rendre visibles des processus interactionnels difficilement accessibles autrement, plutôt que sur leur représentativité quantitative.

La structure de l'association de pairs d'Anonymous

Pour tester correctement la validité de la théorie de l'association différentielle, cette étude a tenté d'observer deux facettes de la théorie : les novices désireux d'apprendre de nouvelles méthodes de piratage et les parrains ou les experts informels désireux d'apporter leur aide. Dans un premier temps, toutes les questions posées ou les demandes impliquant une demande d'aide ou de conseils ont été codifiées. Cela nous a permis d'observer des apprentis Anons désireux d'apprendre des comportements spécifiques associés au piratage :

> [20:32] <UsagerA> J'aimerais que l'on m'explique comment ils ont piraté des sites gouvernementaux.
> (...)
> [04:10] <UsagerB> Où puis-je trouver de bonnes informations sur ce piratage ?

Ce type de question ouverte a donné lieu à des moqueries ou à la dérision pure et simple de leur demande sur l'IRC. Par exemple, l'opérateur d'un forum a exclu un utilisateur du canal à la suite de sa question, puis a fait le commentaire suivant : « Nous n'apprenons pas à pirater quoi que ce soit, le piratage est de l'art, il n'y a que votre tête qui peut apprendre, et elle seule ». Cela suggère que, bien qu'il y ait un accord explicite sur le fait que le piratage est un comportement appris, il n'est pas explicitement enseigné par d'autres pirates, mais est considéré comme un processus d'apprentissage individuel et solitaire.

En revanche, d'autres extraits suggèrent que les néophytes ne sont pas complètement laissés à eux-mêmes dans leur processus d'apprentissage, car d'autres exemples montrent qu'ils tendent à être invités à se tourner vers des ressources tertiaires. Les néophytes sont invités à accéder à des tutoriels sur YouTube et, en outre, à visiter un forum dédié spécifiquement aux individus qui n'ont aucune connaissance informatique et qui souhaitent contribuer aux actions d'Anonymous. Il s'agit du forum #opnewblood et du site web du même nom, opnewblood.fr, qui a été suggéré à plusieurs reprises par des participants. Les personnes n'ayant pas de connaissances informatiques sont donc invitées à se rendre dans ce forum pour poser toutes les questions possibles afin de les aider dans leur processus d'apprentissage :

> [04:10] <UsagerC> Où puis-je trouver de bonnes informations sur le hack ?
> [04:11] <UsagerD> google est le meilleur :)
> (...)
> [19:16] <UsagerE> Pour les noobs [nouveaux arrivants] qui voudraient améliorer leurs connaissances : https://www.youtube.com/watch?v=[masqué]

(...)
[16:11] <UsagerF> Bonjour à tous, je suis nouveau ici et je ne connais pas encore les règles. Y aurait-il une âme charitable qui pourrait m'expliquer comment ça marche si possible ?
[16:12] <UsagerG> vous avez le canal #opnewblood.fr qui pourrait tout expliquer.

Ces passages illustrent les ressources préférées et, en fait, la structure du processus d'apprentissage préféré des personnes n'ayant aucune connaissance en informatique. Dans un état presque contradictoire, les nouveaux arrivants ne reçoivent pas d'aide directe, mais sont encouragés à apprendre par eux-mêmes, même si c'est avec l'aide de ressources tierces et de tutoriels créés par leurs pairs.

L'apprentissage des compétences techniques

Malgré l'accueil au vitriol souvent réservé aux débutants autoproclamés, les conversations fournissent de nombreuses preuves de situations où des Anons expérimentés partagent volontairement leurs compétences techniques et fournissent des ressources et des conseils pour améliorer les compétences d'autres personnes. Il a été observé que certains Anons semblent plus réceptifs à ceux qui ont démontré un minimum de connaissances avant de rejoindre la chambre en posant des questions très spécifiques et concises. Il est certain que le fait de poser des questions ciblées peut être perçu par les Anons plus expérimentés comme une tentative d'affiner des connaissances préexistantes, plutôt que comme l'impression d'inexpérience qui découle de questions générales. Comme l'a mentionné l'un des utilisateurs, les nouveaux venus ne recevront pas d'aide gratuitement ; ils doivent avoir démontré qu'ils ont fait leurs propres recherches et qu'ils ont acquis des connaissances supplémentaires. Ce n'est qu'à ce moment-là que des personnes plus expérimentées seront enclines à compléter leur processus d'apprentissage. Les passages suivants illustrent clairement le mentorat informel dans lequel une question plus approfondie aboutit à une réponse constructive entre les utilisateurs :

[13:20] <UsagerH> on peut enlever la partie proxychains
[13:20] <UsagerI> A quoi ça sert ?
[13:21] <UsagerH> proxychains est une commande utilisée pour filtrer le programme à travers un proxy, vous n'avez probablement pas proxychains installé et vous avez probablement un VPN en cours d'exécution.
(...)
[18:11] <UsagerJ> Quel est le meilleur programme pour une attaque DDoS ?
[18:11] <UsagerK> hping : http://www.hping.org/]-[OS : Linux, FreeBSD, NetBSD, OpenBSD, Solaris, macOS X, Windows - Pour plus d'informations : -hping
[18:11] <UsagerK> Slowloris : http://[édité]-[OS : Linux - Pour plus d'informations : -slowloris
[18:11] <UsagerK> HOIC : http://[édité]]-[OS : Windows - Pour plus d'informations : -hoic

Ces exemples illustrent la demande d'aide telle qu'elle se manifestait au sein des forums d'Anonymous. Cette forme d'apprentissage, qui se résume à l'échange d'opinions et de ressources par d'autres Anons, semble être motivée par le désir d'apprendre de nouvelles méthodes et d'améliorer ses compétences. Cela permet aux pirates d'être continuellement au courant des dernières avancées technologiques. Néanmoins, il est important de noter que l'apprentissage se fait principalement entre pirates expérimentés sous forme d'échange de connaissances, de conseils et de recommandations. Pour les débutants, il y a un renvoi constant vers les ressources tertiaires externes, en particulier le site opnewblood.fr pour les guider dans l'apprentissage des techniques de piratage de base :

[15:47] <UsagerL> Les VPN suivants ont des serveurs localisés en Suède, ce qui devrait garantir votre sécurité.
[15:47] <UsagerL> Utilisez-les à vos risques et périls ! Rien n'est garanti. ET N'UTILISEZ PAS [censuré] UN GRATUIT TON [censuré] Pour plus d'aide sur IRC/ Anonymat, rejoignez #opnewblood.

En accord avec les exemples précédents, ces deux derniers extraits illustrent le fait que certains participants, en manifestant une maîtrise technique à travers des explications détaillées ou la correction des propos d'autrui, adoptent une posture d'« Anons expérimentés » dans le chat. Il apparaît que certains participants sont prompts à aider les autres et contribuent à faire comprendre les nuances du piratage à ceux qui peinent à en saisir les subtilités. Ces conseils sont très spécifiques, et sont basés sur des expériences personnelles passées, car UsagerL les avertit des risques, tout en encourageant les moyens d'atténuer ces risques grâce à des compétences et des connaissances technologiques accrues

L'apprentissage des définitions

L'internalisation de définitions telles que les motivations et les attitudes est cruciale pour l'apprentissage des comportements, car elle encourage les individus à mettre en pratique ces comportements. Notre analyse a mis au jour plusieurs définitions qui augmentent et renforcent la popularité de ces techniques. En particulier, dans les conversations, les Anons 1) rationalisent la conceptualisation de bonnes et mauvaises cibles, 2) créent des rôles et des tâches pour les nouveaux Anons qui aident à renforcer et promouvoir leurs cyberattaques, et 3) célèbrent les pirates habiles, motivant potentiellement d'autres personnes à apprendre des techniques plus complexes.

Tout d'abord, plutôt que d'attribuer une étiquette morale universelle à la technique elle-même, ils catégorisent les cibles, suggérant que l'attaque DDoS peut être bonne si elle est dirigée vers de bonnes cibles et que, de la même manière, la même technique peut être perçue comme mauvaise si elle est utilisée contre une mauvaise cible :

[18:41] <UsagerM> Il faut attaquer de bonnes cibles pour envoyer le bon message.
(...)
[12:09:] <UsagerN> [le département de la police] est une bonne cible
(...)
[19:05] <UsagerO> on n'attaque pas les médias, règle de Anonymous
(...)
[10:15] <UsagerP> Oui, mais rappelons que le conflit

étudiant n'est pas vraiment le sujet ici, Anon, c'est plutôt la liberté d'expression.
(...)
[18:56] <UsagerQ> et le gouvernement s'en prend au peuple

Alors qu'ils sont déconnectés les uns des autres, ces extraits suggèrent que les Anons disposent d'un critère pour déterminer la validité d'un piratage. Ainsi, comme l'affirme UsagerO, attaquer les médias (symbole de la liberté d'expression) n'enverrait pas le bon message, car ils n'oppriment pas activement et explicitement le peuple. Le fait de présenter le gouvernement comme l'oppresseur légitime le comportement, car il permet aux Anons de se considérer comme luttant contre un régime répressif, réagissant aux attaques du gouvernement plutôt que d'initier des attaques contre un gouvernement légitime. Cette justification est renforcée par la honte et la moquerie des pairs observée dans les forums lorsqu'un Anon attaque une mauvaise cible :

[14:25] <UsagerR> Hier, j'ai piraté le site d'une colonie de vacances, la colonie [nom de la colonie de vacances] xD joie !
[14:26] <UsagerS> On s'en fout !
[14:26] <UsagerT> J'espère que tu n'en es pas fier.
[14:28] <UsagerU> Ouais, c'est pas fort...

Dans un autre exemple, un Anon solitaire a piraté une municipalité adjacente sans lien évident avec les évènements du Printemps Érable, s'en vantant dans les forums après coup. Cela a suscité des critiques quant à la raison de l'attaque, la majorité d'entre eux affirmant qu'il s'agissait d'une mauvaise cible et, par conséquent, d'un mauvais comportement. Ce qui caractérise ces cibles comme intrinsèquement mauvaises, c'est qu'elles ne correspondent pas au récit d'une force oppressive attaquant des citoyens ordinaires. Les Anons semblent adhérer à un consensus selon lequel le comportement lui-même a des limites morales, concernant son utilisation acceptable uniquement contre de « bonnes » cibles oppressives. Ceux qui n'adhèrent pas à cette logique sont soumis à des formes d'humiliation de la part d'autres, ce qui encourage fortement une conformité future dans l'utilisation du comportement par le délinquant et les autres témoins de l'humiliation en ligne. Même si ce n'est peut-être pas l'objectif principal, cela encourage involontairement la cohérence dans la sélection des cibles.

Deuxièmement, les attitudes légitimant l'utilisation des techniques de piratage sont soutenues et renforcées par la promotion des attaques réussies sur les médias sociaux. D'après les analyses, les échanges suggèrent qu'un certain nombre d'usagers rejoignent le chat par intérêt pour la cause, que ce soit simplement pour encourager les autres Anons dans leurs actions, ou par désir de s'impliquer. Plusieurs commentaires ont montré un schéma similaire où leur volonté de s'impliquer était contrebalancée par leur manque de compétences technologiques. Par conséquent, les Anons présents sur le chat se sont empressés d'attribuer un rôle à ces personnes :

[17:18] <UsagerU> Bonjour. Je suis nouvelle ici. J'aimerais aider pour la cause même si j'ai le niveau de compréhension informatique d'une grand-mère.
(...)
[17:54] <UsagerV> en tant que nouvel arrivant, j'aimerais savoir ce que nous pouvons faire en temps voulu pour pouvoir participer.
(...)
[21:18] <UsagerW> ceux qui ne sont pas Ace [bon] dans le hacking peuvent quand même être utiles dans la propagande sur twitter, facebook,... distribuer des vidéos et des images autant que possible.

Le commentaire de UsagerW est impératif pour comprendre la promotion et le renforcement positif de ces comportements parmi ceux qui participent aux chats. Connus sous le nom « d'assertion », les hacktivistes utilisent les médias sociaux pour se vanter publiquement d'une attaque de piratage réussie et informer le public des différentes causes politiques sociales avec lesquelles il est actuellement engagé (George et Leidner, 2019). Dans le cadre de la théorie de l'association différentielle, le fait de permettre aux Anons qui n'ont pas les compétences nécessaires pour pirater de s'engager dans l'affirmation contribue à favoriser la solidarité entre tous ses membres, en amenant les utilisateurs à promouvoir les attaques sur leur propre profil de média social, renforçant ainsi leurs perspectives du comportement de piratage comme étant légitimes. Elle approuve l'utilisation des techniques de piratage, ce qui peut contribuer à la normalisation et à la légitimation continue de ces comportements pour ceux qui cherchent à y participer.

Enfin, les Anons qui participent aux chats promeuvent un point de vue qui attribue un système de valeurs aux méthodes de piratage les plus populaires. Cette hiérarchie s'articule autour de la facilité avec laquelle le piratage est effectué et de son effet/impact sur les cibles données. Au cours de l'opération Québec, les conversations relatives au lancement d'une attaque portaient par défaut sur l'utilisation d'attaques DDoS, car elles étaient faciles à réaliser et donc accessibles à tous ceux qui souhaitaient y participer, quel que soit leur niveau de compétence. À l'inverse, les conversations autour des attaques DDoS n'ont pas été unanimement glorifiées, mais ont souvent suscité des critiques et de l'insatisfaction :

[19:09] <UsagerX> du DDoS maintenant n'importe qui peut le faire.
(...)
[18:58] <UsagerY> Un DDoS n'est pas un hack.
(...)
[20:59] <UsagerZ> le DDoS c'est rien, le defacing ça demande plus de talent.
(...)
[21:56] <UsagerAA> Le DDoS est une attaque pour occuper les nouveaux, souvent inutiles et peu fiables, et surtout risqués)...comment aider ?
(...)
[20:26] <UsagerAB> Je crois qu'un deface a un impact BCP +.
(...)
[20:02] <UsagerAC> J'avoue que le défigurage, j'adore ça

Ces opinions argumentent que les attaques DDoS ne sont pas considérées comme une technique de piratage basé sur une perspective qui la caractérise comme inutile, peu fiable et improductive. Bien qu'aucune justification explicite de ces opinions ne soit donnée, le concept d'impact imprègne le discours entourant ces opinions convergentes, même si c'est de manière implicite. L'impact perçu comme plus important associé à la dégradation, ainsi que l'appréciation enthousiaste observée par l'usagerAB et l'usagerAC respectivement, fait ressortir la valeur des différentes techniques pour tous ceux qui ont participé aux discussions. Ces points de vue n'ont fait l'objet d'aucune réaction négative ou dissidente, ce qui signifie que, même si le DDoS est populaire, l'utilisation de la défiguration de sites web jouit d'un plus grand respect, car elle a un impact perçu plus important et est donc considérée comme une technique de piratage supérieure à son prédécesseur. Par conséquent, le piratage et le pirate sont liés, les piratages complexes étant représentatifs d'un pirate habile, ce qui entraine également des distinctions entre les Anons:

> [22:04] <UsagerAD> C'est toi moi...ou le DDoS ne donne rien ! Il n'y a que les vrais Anonymous qui peuvent pirater pour de vrai ? Je ne pense même pas que nous soyons utiles.
> (...)
> [22:33] <UsagerAE> en espérant que des defacers apparaissent, je n'ai pas les compétences pour ça (malheureusement).

Ces commentaires créent un environnement qui encourage implicitement un plus grand développement en faisant explicitement l'éloge de ceux qui peuvent utiliser la défiguration de sites web comme étant supérieur aux autres membres. En associant l'apprentissage des techniques de piratage à un talent, on sous-entend que ce type de technique de piratage fait partie d'un club exclusif de pirates. Pour certains, comme l'illustre l'usagerAE, cela peut les dissuader d'essayer d'améliorer leurs connaissances et leurs compétences en raison de la perception qu'ils ont de leurs compétences actuelles. Cependant, le respect et la révérence associés à ceux qui se livrent à des piratages plus complexes peuvent encourager les nouveaux venus à apprendre des techniques plus efficaces s'ils souhaitent être considérés comme de véritables membres d'Anonymous et abandonner les techniques considérées comme des tâches fastidieuses. En renforçant l'idée que les techniques plus simples ne font pas d'un individu un pirate, et peuvent avoir un impact négatif sur son appartenance au groupe, la culture qui entoure les conversations est une culture qui fournit des motivations pour une croissance continue parmi les individus qui souhaitent maîtriser ces compétences particulières.

L'interprétation des résultats

L'application de la théorie de l'association différentielle à l'étude d'Anonymous permet de tirer certaines conclusions concernant l'environnement en ligne des campagnes de piratage et son impact sur le processus d'apprentissage des nouvelles recrues. Tout d'abord, de nombreux exemples contredisent l'affirmation selon laquelle les nouveaux venus ne reçoivent aucune aide de leurs pairs en ligne. Par rapport aux groupes de pirates informatiques traditionnels et à la connaissance préalable des campagnes Anonymous, une grande partie des membres étaient des nouveaux venus à la recherche de conseils, souhaitant participer à une opération de piratage pour la première fois (Babko-Malaya et al., 2017 ; Coleman, 2020). Bien que nous ne puissions pas exclure une certaine hostilité envers ce sous-groupe de participants, la redirection vers des ressources en ligne préétablies et des forums d'aide pour novices, suggère que les forums IRC analysés sont, tout au moins, adjacents à un environnement susceptible de favoriser le processus d'apprentissage des individus. Bien que cela aurait pu éliminer le besoin d'une forme de parrain individuel, les extraits présentés mettent en évidence des cas où des Anons plus expérimentés transmettent leurs connaissances et expériences à ceux qui démontrent un certain niveau de connaissances à priori. Ces observations valident la présence d'un environnement adapté au processus d'apprentissage des individus par la communication et la transmission des compétences techniques nécessaires à l'apprentissage des subtilités de l'exécution de ces comportements, comme le souligne la théorie de l'association différentielle.

Deuxièmement, l'association différentielle affirme qu'un comportement est appris lorsque les définitions favorables à son utilisation l'emportent sur celles qui le rejettent. Les recherches sur les groupes de pairs adolescents ont montré que la critique, la désignation d'un bouc émissaire et la honte sont utilisées pour imposer la conformité aux membres, cette autorité sur le comportement étant due au besoin d'appartenance des individus (Laninga-Wijnen et Veenstra, 2021 ; Laursen et Veenstra, 2021). En raison de ce besoin de conformité, les individus qui ne se conforment pas risquent d'être punis pour leurs actes, voire d'être complètement ostracisés. Nous avons observé le cas de l'utilisation de proposition de s'attaquer à de « mauvaises » cibles. Nous avons observé que des discussions ont permis aux nouvelles recrues d'apprendre aussi bien la différence entre une bonne ou une mauvaise cible, mais aussi de voir les répercussions pour ceux qui n'adhèrent pas aux valeurs du groupe. Comme l'ont montré Fortin et al. (2022), l'apprentissage hacktiviste inclut non seulement la transmission de savoir-faire techniques, mais aussi l'internalisation de définitions et de normes collectives, ce qui rejoint directement les dynamiques observées dans notre corpus. Certains peuvent intérioriser les définitions d'une manière erronée, en ciblant par erreur une mauvaise cible, ce qui pourrait expliquer la vantardise observée par un Anon qui a piraté un camp de jour, à la consternation des autres.

La promotion de techniques de piratage plus complexes peut également contribuer au processus d'apprentissage des néophites. En associant la défiguration de sites Web à un plus grand respect et acceptation de la part des autres membres, les nouveaux venus sur les chats peuvent intérioriser ces motivations. L'inclusion de cetter définition dans les forums va dans le même sens que les conclusions précédentes, car elle s'appuie sur le besoin de conformité et de reconnaissance pour garantir l'uniformité.

Enfin, le rôle de l'affichage sur les médias sociaux est souvent laissé aux nouveaux venus et aux néophytes, qui en tirent une satisfaction. Dans l'association différentielle, le processus d'apprentissage est renforcé par la durée, l'intensité et la répétition de définitions qui se renforcent elles-mêmes. En continuant à publier des contenus d'Anonymous en ligne, les

utilisateurs des médias sociaux ne font que renforcer et intérioriser leur approbation des cyberattaques d'Anonymous. Bien que cette conclusion n'ait pas encore été développée dans la littérature consacrée aux pirates informatiques, l'utilisation des médias sociaux pour renforcer les valeurs et les actions d'un groupe a été documentée dans la recherche sur le cyberterrorisme (Hollewell et Longpré, 2022) et sur les gangs de rue (Campisi, 2019).

L'objectif de cette étude était de comprendre les interactions entre les membres d'Anonymous lors d'une campagne de piratage, afin de déterminer si cela peut expliquer comment de nouveaux Anons apprennent régulièrement des techniques similaires pour cibler des entités similaires. Alors que l'utilisation de ressources tertiaires suggère qu'elles offrent un environnement propice à l'apprentissage et au renforcement des valeurs, l'observation de l'apprentissage des bonnes et des mauvaises cibles montre qu'elles fournissent aussi une motivation pour apprendre le piratage de sites Web. En promouvant des activités qui favorisent l'adhésion au groupe (par le contenu diffusé sur les médias sociaux), elles permettent de comprendre comment Anonymous a mobilisé les mêmes techniques contre des cibles similaires pendant plus de dix ans de campagnes.

Les limites de l'étude

L'objectif de la présente étude était d'appliquer l'association différentielle dans le contexte du hacktivisme pour en apprendre davantage sur les mécanismes de l'apprentissage au sens où Sutherland *et al.*, (1992) le suggère. Cette étude n'est pas sans limites. D'abord, par rapport aux recherches actuelles sur le groupe hacktiviste, cette étude n'analyse pas les comptes de médias sociaux, car son objectif est de comprendre comment l'apprentissage des techniques de piratage, les motivations, les cognitions, etc., se développent dans de forums plus clandestins et plus privés. Il ne fut donc pas possible de mesurer l'impact que les médias sociaux pourraient avoir dans l'apprentissage, notamment en termes de rationalisation pour l'adhésion à certaines causes. Deuxièmement, les données issues de l'opération Québec permettent d'avoir une compréhension fondamentale de l'association entre pairs d'Anonymous en utilisant des données de conversations entre participants, données souvent difficiles à obtenir (Coleman, 2020). Elles permettent de savoir et de connaître les motivations manifestées devant les autres, mais elle n'est certainement pas l'équivalent d'un test psychométrique, puisque de nombreux mécanismes font obstacle à la pensée réelle des auteurs. De plus, l'étude s'appuie sur une approche exclusivement qualitative : les extraits présentés visent à illustrer des dynamiques récurrentes sans prétendre à une représentativité statistique. L'absence de quantification systématique (par exemple, du nombre exact de demandes d'aide ou de la proportion d'utilisateurs redirigés vers des ressources tertiaires) limite la possibilité d'évaluer l'ampleur relative des phénomènes observés. Ainsi, les résultats doivent être interprétés comme une analyse en profondeur de processus sociaux plutôt que comme une mesure de fréquence.

Finalement, ces conclusions découlent de l'utilisation de données datant de 2012. L'opération Québec s'est déroulée il y a plus d'une décennie et plusieurs dizaines de campagnes ont eu lieu depuis. Ces conclusions doivent être considérées comme un point de référence initial, encourageant la reproduction future de cette analyse à travers différentes campagnes à différents moments. Les forums analysés n'ont révélé aucune indication claire qui a créé et organisé les ressources tertiaires observées, et ne peut donc pas affirmer avec certitude que chaque campagne individuelle utilise ces mêmes ressources. Cependant, compte tenu des années de campagnes homogènes, les conclusions présentées offrent la première explication plausible quant à la capacité des groupes décentralisés à apprendre et à utiliser les mêmes techniques de piratage.

Conclusion

En conclusion, l'application de la théorie de l'association différentielle à l'étude d'Anonymous révèle des éléments significatifs sur l'environnement en ligne des campagnes de piratage et son impact sur le processus d'apprentissage des nouveaux membres. D'une part, les néophytes semblent avoir l'opportunité de bénéficier de conseils et de ressources en lignes, suggérant que les forums IRC analysés peuvent favoriser le processus d'apprentissage. D'autre part, les normes du groupe, ses cibles favorites et les techniques fréquemment utilisées sont renforcées via des interactions en ligne via la promotion de techniques complexes et l'instauration d'une moralité. Enfin, les médias sociaux renforcent l'approbation des cyberattaques d'Anonymous.

Des recherches futures doivent reproduire l'étude dans différents contextes et campagnes pour mieux comprendre le processus d'apprentissage des hacktivistes. Avec l'augmentation de la fréquence des campagnes d'Anonymous, une priorité accrue doit être accordée à la compréhension du processus d'apprentissage des hacktivistes désireux de cibler les entités gouvernementales. En complément, l'intégration d'une dimension quantitative viendrait enrichir l'approche qualitative retenue ici, en permettant par exemple d'estimer la proportion de messages consacrés à certains types de cibles, de comparer la fréquence de l'aide accordée aux néophytes et aux membres expérimentés, ou encore de mesurer la répartition des discussions entre différentes thématiques. Par ailleurs, l'analyse pourrait être élargie à d'autres plateformes, notamment les réseaux sociaux, afin d'examiner le rôle de ces espaces publics dans la mise en valeur des attaques, et ainsi mieux comprendre l'articulation entre coordination en ligne et communication externe.

Références

Anderson, N. (2012, 4 mai). Literally the day he was arrested, hacker "Sabu" helped the FBI [Nouvelles]. *Ars Technica*. https://arstechnica.com/tech-policy/news/2012/05/literally-the-day-of-his-arrest-hacker-sabu-helped-the-fbi.ars

Babko-Malaya, O., Cathey, R., Hinton, S., Maimon, D., et Gladkova, T. (2017). Detection of hacking behaviors and communication patterns on social media. *Big Data*, 4636–4641.

Bardeau, F., et Danet, N. (2011). *Anonymous: Pirates informatiques ou altermondialistes numériques? : Peuvent-ils changer le monde ?* Éditions FYP.

Bégin-Caouette, O., et Jones, G. A. (2014). Student organizations in Canada and Quebec's 'Maple Spring.' *Studies in Higher Education*, 39(3), 412–425. https://doi.org/10.1080/03075079.2014.896178

Beraldo, D. (2022). Unfolding #Anonymous on Twitter: The networks behind the mask. *First Monday*, 27(1), n.p. https://dx.doi.org/10.5210/fm.v27i1.11723

Bergeron, A., Delle Donne, J., et Fortin, F. (2019). Une publication pour dénoncer, sans plus: description des activités des groupes Facebook s'identifiant au mouvement Anonymous au Canada. *La criminologie de l'information : état des lieux et perspectives*, 52(2), 35–62. http://doi.org/10.7202/1065855ar

Bodó, B. (2014). Hacktivism 1-2-3: How privacy enhancing technologies change the face of Anonymous hacktivism. *Internet Policy Review*, 3(4), 1–13.

Caldwell, T. (2015). Hacktivism goes hardcore. *Network Security*, 5, 12–17. https://doi.org/10.1016/S1353-4858(15)30039-8

Campisi, F. (2019). From the streets to the tweets: Social network analysis of Canadian street gang members and their use of Twitter, Facebook and YouTube [Thèse de Maîtrise, L'université Queens]. https://www.proquest.com/docview/2371722209?pq-origsite=gscholar&fromopenview=true

CBC News. (2012, 20 avril). Violent Montreal student protest nets 17 arrests [Nouvelles]. CBC. https://www.cbc.ca/news/canada/montreal/violent-montreal-student-protest-nets-17-arrests-1.1139959

Chen, X., et Wang, H. (2019). Automated chat transcript analysis using topic modeling for library reference services. *Proceedings of the Association for Information Science and Technology*, 56, 368–371.

Coleman, E. G. (2020). Logics and legacy of Anonymous. Dans J. Hunsinger, M. Allen, et M. Klastrup (éds.), Second international handbook of internet research. *Springer*.

Coleman, G. (2014). *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous.* Verso.

Daudens, F. (2012, 21 mai). *Les Anonymous piratent plusieurs sites du gouvernement du Québec | Blogue des chroniques Sur le web | Radio-Canada.ca* [Blog]. Radio Canada.ca. https://web.archive.org/web/20130822085752/http://blogues.radio-canada.ca/surleweb/2012/05/21/anonymous-operation-quebec/

de la Hamaide, S. (2015, 14 novembre). *Timeline of Paris attacks according to public prosecutor* [Nouvelles]. Reuters. https://www.reuters.com/article/us-france-shooting-timeline-idUSKCN0T31BS20151114

Décary-Hétu, D. (2014). Information exchange paths in IRC hacking chatrooms. Dans *Crime and networks* (pp. 218–230). Routledge.

Décary-Hétu, D., et Leppänen, A. (2013). Criminals and signals: An assessment of criminal performance in the carding underworld. *Security Journal*, 29(3), 442–460.

Dobusch, L., et Schoeneborn, D. (2015). Fluidity, identity, and organizationality: The communicative constitution of Anonymous. *Journal of Management Studies*, 52(8), 1005–1035. https://doi.org/10.1111/joms.12139

Fortin, F., Campisi, F. C., et Néron, M.-È. (2022). Hacktivism from the inside: Collective identity, target selection and tactical use of media during the Québec maple spring protests. *Rivista Di Criminologia, Vittimologia e Sicureza*, 16(1), 35–56. https://doi.org/10.14664/rcvs/242

Gagnon, A. (2018). Extending social learning theory to explain victimization among gang and ex-gang offenders. *International Journal of Offender Therapy and Comparative Criminology*, 62(13), 4124–4141. https://doi.org/10.1177/0306624X18763761

George, J. J., et Leidner, D. E. (2019). From clicktivism to hacktivism: Understanding digital activism. *Information and Organization*, 29(3), 1–45. https://doi.org/10.1016/j.infoandorg.2019.04.001

Géring, Z. (2021). Mixed methodological discourse analysis. Dans A. J. Onwuegbuzie et R. B. Johnson (éds.), *The Routledge reviewer's guide to mixed methods analysis* (pp. 161–172). Routledge.

Guiton, A. (2013). *Pirates: au cœur de la resistance numérique*. Éditions Au diable Vauvert.

Gunkel, D. J. (2005). Editorial: Introduction to hacking and hacktivism. *New Media & Society*, 7(5), 595–597. https://doi.org/10.1177/1461444805056007

Hollewell, G. F., et Longpré, N. (2022). Radicalization in the social media era: Understanding the relationship between self-radicalization and the Internet. *International Journal of Offender Therapy and Comparative Criminology*, 66(8), 896–913. https://doi.org/10.1177/0306624X211028771

Jones, K., Nurse, J. R. C., et Li, S. (2020). Behind the mask: A computational study of Anonymous' presence on Twitter. *Proceedings of the Fourteenth International AAAI Conference on Web and Social Media* (ICWSM 2020), 14, 327–338.

Jul, C. (2013, 30 juillet). *Hacktivism & Anonymous* [Blog]. Calum Stuart. http://calumstuart.com/hacktivism-anonymous/

Kelly, B. B. (2012). Investing in a centralized cybersecurity infrastructure: Why hacktivism can and should influence cybersecurity reform note. *Boston University Law Review*, 92(5), 1663–1712. https://heinonline.org/HOL/P?h=hein.journals/bulr92&i=1685

Kenney, M. (2015). Cyber-terrorism in a Post-Stuxnet world. *Orbis*, 59, 111–128. https://doi.org/10.1016/j.orbis.2014.11.009

Klein, A. G. (2015). Vigilante media: Unveiling Anonymous and the hacktivist persona in the global press. *Communication Monographs*, 82(3), 379–401.

Laninga-Wijnen, L., et Veenstra, R. (2021). Peer similarity in adolescent social networks: Types of selection and influence, and factors contributing to openness to peer influence. Dans B. Halpern-Felsher (éd.), *The encyclopedia of child and adolescent health* (pp. 2–39). Elsevier.

Laursen, B., et Veenstra, R. (2021). Toward understanding the functions of peer influence: A summary and synthesis of recent empirical research. *Journal of Research on Adolescence*, 31(4), 889–907. https://doi.org/10.1111/jora.12606

Léger, M. J. (2019). *Vanguardia: Socially engaged art and theory*. Manchester University Press.

Levesque, C. (2012, 20 mai). *Grève étudiante: un vidéo d'Anonymous dénonce la loi 78 et lance l'opération Québec* [Nouvelles]. HuffPost Québec. https://quebec.huffingtonpost.ca/2012/05/20/anonymous-operation-quebec_n_1531489.html

Levin, R., Richardson, J., Warner, G., et Kerley, K. (2012). Explaining cybercrime through the lens of differential association theory, Hadidi44-2.php PayPal Case Study. *eCrime Research Summit*, 1–7. https://doi.org/10.1109/eCrime.2012.6489518

Li, X. (2013). Hacktivism and the first amendment: Drawing the line between cyber protests and crime. *Harvard Journal of Law & Technology*, 27(1), 302–329. https://heinonline.org/HOL/Page?handle=hein.journals/hjlt27&div=10&g_sent=1&casa_token=lBHXqKfp3kAAAAAA:OEsXVx62wbMXVHDCOZihtTqFYcv5-Oj5AKSE_-14MUcnXxVf5lGKnerbMEpUi16eyagEq4wr&collection=journals

Machado, M. B. (2015). Between control and hacker activism: The political actions of Anonymous Brazil. *Historia, Ciencias, Saude--Manguinhos*, 22, 1531–1549. http://dx.doi.org/10.1590/S0104-59702015000500002

Mansfield-Devine, S. (2011). Anonymous: Serious threat or mere Annoyance? *Network Security*, 1, 4–10. https://doi.org/10.1016/S1353-4858(11)70004-6

Marcum, C. D., Higgins, G. E., Ricketts, M. L., et Wolfe, S. E. (2014). Hacking in high school: Cybercrime perpetration by juveniles. *Deviant Behavior*, 35(7), 581–591. https://doi.org/10.1080/01639625.2013.867721

McGovern, V., et Fortin, F. (2019). The Anonymous collective: Operations and gender differences. *Women & Criminal Justice*, 30(2), 1–15. https://doi.org/10.1080/08974454.2019.1582454

Molloy, D., et Tidy, J. (2020, 1 juin). George Floyd: Anonymous hackers re-emerge amid US unrest. *BBC News*. https://www.bbc.com/news/technology-52879000

Morris, R. (2011). Computer hacking and the techniques of neutralization: An empirical assessment. Dans *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications, IGI Global*, 1–17. https://doi.org/10.4018/978-1-61692-805-6.ch001

Morris, R. G., et Blackburn, A. G. (2009). Cracking the code: An empirical exploration of social learning theory and computer crime. *Journal of Crime and Justice*, 32(1), 1–34. https://doi.org/10.1080/0735648X.2009.9721260

Morris, R. G., et Higgins, G. E. (2010). Criminological theory in the digital age: The case of social learning theory and digital piracy. *Journal of Criminal Justice*, 38(4), 470–480. https://doi.org/10.1016/j.jcrimjus.2010.04.016

Morselli, C., Tremblay, P., et Mccarthy, B. (2006). Mentors and criminal achievement*. *Criminology*, 44(1), 17–43. https://doi.org/10.1111/j.1745-9125.2006.00041.x

Olsen, P. (2012). *We are Anonymous: Inside the hacker world of LulzSec, Anonymous, and the global cyber insurgency*. Back Bay Books.

Purtill, J. (2022, 24 février). *Anonymous takes down Kremlin, Russian-controlled media site in cyber attacks* [Nouvelles]. ABC News. https://www.abc.net.au/news/science/2022-02-25/hacker-collective-anonymous-declares-cyber-war-against-russia/100861160

Raynauld, V., Lalancette, M., et Tourigny-Koné, S. (2016). Political protest 2.0: Social media and the 2012 student strike in the province of Quebec, Canada. French Politics, 14(1), 1–29. https://doi.org/10.1057/fp.2015.22

Renzi, A. (2015). Info-capitalism and resistance: How information shapes social movements. *Interface: A Journal for and about Social Movements*, 7(2), 98–119.

Schrock, A. R. (2016). Civic hacking as data activism and advocacy: A history from publicity to open government data. *New Media & Society*, 18(4), 581–599. https://doi.org/10.1177/1461444816629469

Steinmetz, K. F. (2022). Hacking and hacktivism. Dans R. Atkinson et T. Ayres (éds.), *Shades of Deviance: A Primer on Crime, Deviance and Social Harm* (2e éditon.). Taylor & Francis.

Sutherland, E. H., Cressey, D. R., et Luckenbill, D. F. (1992). *Principles of criminology*. Rowman & Littlefield Publishers.

Warr, M., et Stafford, M. (1991). The influence of delinquent peers: What they think or what they do?*. *Criminology*, 29(4), 851–866. https://doi.org/10.1111/j.1745-9125.1991.tb01090.x