UNIVERSITÉ DU QUÉBEC À MONTRÉAL

COMMENT LA SÉRIE *HACKERS* COMMUNIQUE, SENSIBILISE ET ÉDUQUE SUR LES GRANDS ENJEUX TOUCHANT LA CYBERCRIMINALITÉ ET LES IDENTITÉS NUMÉRIQUES

MÉMOIRE
PRÉSENTÉ
COMME EXIGENCE PARTIELLE
DE LA MAÎTRISE EN COMMUNICATION

PAR
SARA NACER

MARS 2018

REMERCIEMENTS

Je tiens à témoigner ma gratitude à toutes les personnes qui ont participé à la réalisation de ce travail.

Tout d'abord à mon directeur de mémoire, Claude-Yves Charron, qui a accepté de me suivre dans la concrétisation de ce projet de recherche. Ses précieux conseils, sa bienveillance, son soutien indéfectible tout au long de la réalisation de ce mémoire m'ont permis de mener à bien ce travail.

Merci également aux membres de mon jury, Pierre-Léonard Harvey et Yves Théoret, dont les conseils m'ont permis d'approfondir ma recherche et la réflexion qu'elle a entraînée.

Mes sincères remerciements à mes parents, à mon frère et à mes proches pour leur soutien.

« Froide ou chaude, la prochaine guerre sera cyber »
Le Nouvel Observateur, 2016

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES TABLEAUX

RÉSUMÉ

Dans un monde « hyperconnecté », les enjeux relatifs à la cybersécurité et à la protection des identités numériques deviennent une importante préoccupation. Ce travail de recherche soulève la problématique du rôle des communications dans l'éducation, et tente d'évaluer la sensibilisation du public à ces enjeux. C'est par une étude de la réception de la série documentaire *Hackers,* représentative des productions télévisuelles contemporaines, que nous tenterons de comprendre comment ces différents enjeux peuvent être perçus.

Mots clés : Cybersécurité, communication, réception, identités numériques, *hacking*

INTRODUCTION

Internet est aujourd'hui reconnu comme un outil de communication incontournable, et cela, à l'échelle mondiale. Au Québec, conscient de l'importance de cet outil de communication, de son impact sur les performances des entreprises et sur la croissance économique de la province, le gouvernement a mis en place, par l'entremise de son ministère de l'Économie, de la Science et de l'Innovation, sa « Stratégie numérique ». Il s'agit d'un grand chantier dont le but est de « définir une vision gouvernementale cohérente afin que le Québec évolue vers une société numérique[1] ». Le ministère a d'ailleurs procédé à une large consultation publique afin que « cette stratégie [soit] élaborée en collaboration avec les citoyens, les experts, les entreprises et les organisations, selon leurs préoccupations, leurs besoins, leurs réflexions et leurs idées[2] ».

À l'échelle de l'individu, Internet a véritablement révolutionné nos habitudes de communication et nos interactions sociales avec l'émergence de l'identité numérique. Cette dernière, devenue l'élément de base de nos interactions, est définie comme

---

[1] Cabinet de la Ministre de l'Économie, de la Science et de l'Innovation (2017). *Stratégie québécoise de la recherche de l'innovation 2017-2022* [communiqué]. Récupéré de *https://www.economie.gouv.qc.ca/fileadmin/contenu/documents_soutien/strategies/recherche_innovation/SQRI/sqri_complet_fr.pdf*

[2] *Ibid.*

étant *« une transposition graphique, sonore et visuelle d'une représentation en pensée façonnée par le Sujet dans le matériau de l'interface.*[3]*»*

Internet a également transformé nos habitudes de consommation avec *l'internet des objets,* qui regroupe l'ensemble des « objets ayant des identités et des personnalités virtuelles, opérant dans des espaces intelligents et utilisant des interfaces intelligentes pour se connecter et communiquer au sein de contextes d'usages variés[4] ». Avec l'évolution d'Internet, l'émergence de ces deux concepts, l'internet des objets et les identités numériques, témoigne du développement de la sémiotique concernant ses différents usages. Ce nouveau champ d'analyse est une preuve de l'intérêt porté par la recherche contemporaine au développement de ces nouveaux modes de communication.

Outre cet intérêt des chercheurs, nous avons pleinement conscience de l'importance d'Internet et l'avons intégré dans notre quotidien. Mais, si nos gouvernements mettent aujourd'hui en place des politiques visant à faciliter son accessibilité à un maximum de personnes, qu'en est-il des enjeux de cybersécurité forcément reliés à son utilisation ? Quelles sont nos connaissances des risques auxquels Internet nous expose ? Nos identités numériques sont-elles protégées ? Nos habitudes de consommation sont-elles sécuritaires ? Avons-nous conscience des brèches du système, et des dangers auxquels nous sommes exposés ? On s'accorde généralement sur l'importance de faciliter l'accès à l'Internet, mais qu'en est-il de l'importance de sécuriser nos pratiques ? Sommes-nous conscients de la quantité d'informations que nous révélons quotidiennement sous nos identités numériques ? N'est-il pas aussi

---

[3] Georges, Fanny. (2009) *Représentation de soi et identité numérique. Une approche sémiotique et quantitative de l'emprise culturelle du web 2.0 », Réseaux,* 2009/2 (n° 154), p. 165-193. DOI : 10.3917/res.154.0165. *https://www.cairn.info/revue-reseaux-2009-2-page-165.htm*

[4] Benghozi, P.-J. Bureau, S. et Massit-Follea, F. (2012) *L'internet des objets : quels enjeux pour l'Europe,* Paris : Éditions de la Maison des sciences de l'homme. Tiré de http://books.openedition.org/

important de souligner la nécessité de se protéger que de promouvoir l'utilisation d'Internet ? Comment répandre les bonnes pratiques auprès des usagers ? La série *Hackers*, produite en 2016 et qui s'est donné cette mission, peut-elle avoir un impact réel sur notre conscience des dangers présents dans le cyberespace ? Ce sont là des questions auxquelles nous tenterons de répondre dans ce mémoire.

CHAPITRE I

PROBLÉMATIQUE D'ENSEMBLE

Dans cette première partie, nous présenterons notre objet de recherche : une série télévisée qui, parce que diffusée par un canal spécialisé, a une portée limitée. Nous nous intéresserons au rôle que cette série peut jouer dans notre compréhension des implications du partage de données par Internet et de nos multiples interactions sociales virtuelles. Également, nous nous intéresserons aux messages communiqués par ce média et comment ils peuvent influencer notre perception des dangers auxquels nous nous exposons par notre présence dans le cyberespace. Et, comme notre objet d'étude n'est pas un média de masse mais un média spécialisé, nous nous intéresserons davantage au contenu des messages et à leur perception plutôt qu'à leur portée. Par la série *Hackers,* nous tenterons de comprendre comment un média de communication peut être porteur de messages clés qui peuvent sensibiliser son audience et influencer ses pratiques en ligne. Dans un monde où l'hyperconnectivité devient la norme, nous tenterons de comprendre comment une série peut informer, sensibiliser et éduquer de façon que nos pratiques en ligne soient plus sécuritaires et que nous prenions les moyens de protéger nos identités numériques et, par le fait même, notre vie privée. Évidemment, afin de préciser la terminologie relative à notre objet d'étude, nous reviendrons sur les concepts clés de notre analyse : « identités numériques », « internet des objets », « hyperconnectivité », « cyberespace », « cyberattaque » et « cybersécurité ». Finalement, nous poserons la question centrale de notre recherche et formulerons notre hypothèse d'ensemble, en tentant de

déterminer la pertinence de ce mémoire dans le domaine d'étude de la communication internationale.

1.1 Internet

Internet est présent partout. L'agence de marketing américaine We Are Social estime qu'aujourd'hui, sur les 7,476 milliards d'habitants de la Terre, on dénombre 377 milliards[5] d'internautes, soit 50 % de la population mondiale, dont 2,91 milliards[6] sont inscrits sur les réseaux sociaux[7], soit 39 % de la population. Quant au taux de pénétration d'Internet dans le monde, il est notamment de 88 %[8] en Amérique du Nord et de 84 % en Europe de l'Ouest. Le Québec fait donc partie des régions présentant le plus haut taux de pénétration. Selon le Centre facilitant la recherche et l'innovation dans les organisations (CEFRIO), « 90 % des ménages de la province sont branchés – une hausse de 14 points de pourcentage depuis cinq ans.[9] ».

1.1.1 Les réseaux sociaux

Si, à ses débuts, Internet était principalement utilisé pour des usages professionnels ou académiques, aujourd'hui son usage est massivement répandu et il n'est plus voué uniquement au courriel et à la collecte d'informations sur les moteurs de recherche.

---

[5] Le media des professionnels du digital. (2017) *Chiffres Internet – 2017.* Récupéré de https://www.blogdumoderateur.com/chiffres-internet/

[6] *Ibid.*

[7] « Nous définissons les sites de réseaux sociaux en tant que services web qui permettent aux individus de (1) construire un profil public ou semi-public, dans un système borné, (2) articuler une liste d'autres utilisateurs [les « amis » sur Facebook] avec lesquels ils partagent un lien, et (3) voir et arpenter leur liste de liens et celles établies par d'autres au sein du système. La nature et la nomenclature de ces liens peuvent varier d'un site à l'autre » (BOYD et ELLISON 2008, p. 211 — traduction).

[8] *Op. cit.*

[9] Radio-Canada International (2016). *Internet à domicile : le Québec de plus en plus connecté.* Récupéré de http://www.rcinet.ca/fr/2016/11/03/internet-a-domicile-le-quebec-de-plus-en-plus-connecte/

En effet, les réseaux sociaux sont devenus l'espace de socialisation par excellence : Facebook, Instagram, Twitter, Snapchat ou encore Instagram occupent une place centrale dans la vie des utilisateurs d'Internet. À ce sujet, voici quelques chiffres qui démontrent l'importante quantité d'informations partagées sur ces réseaux, mais également le haut niveau d'interaction qu'on y trouve. Selon une étude américaine récente, chaque minute sur Internet il y aurait :

- 7 millions de *snaps* envoyés sur Snapchat
- 216 millions de photos « aimées » sur Facebook
- 2,4 millions de photos « aimées » sur Instagram
- 350 000 *tweets* sur Twitter, dont 10 000 contenant un émoji
- 400 heures de vidéos téléchargées sur YouTube
- 10 000 images épinglées sur Pinterest
- 18 000 *upvotes* ou *downvotes* sur Reddit
- 1 million de vues sur Vine
- 110 000 appels sur Skype
- 70 millions de mots traduits sur Google Translate
- 830 000 fichiers téléchargés sur Dropbox
- 570 000 GIF visionnés issus de Giphy
- 3,5 millions de textos envoyés aux États-Unis [10]

Ces chiffres provenant de l'agence de marketing américaine We Are Social démontrent clairement que nos habitudes de communication ont muté avec le développement d'Internet, et que les réseaux sociaux occupent une place centrale dans nos interactions sociales.

---

[10] *Op. cit.*

1.1.2 L'hyperconnectivité

Dans une revue de presse, on trouve un grand nombre d'articles qui traitent des dangers d'Internet pour la santé. Le site danger-sante.org, par exemple, regroupe différents articles traitant des dangers d'Internet et des effets néfastes de notre surexposition aux ondes Wi-Fi. De très nombreuses études traitant du même sujet sont aussi parues dans des journaux. Récemment, le journal turc *Daily Sabah,* dans la section Health (Santé) de son édition du 9 août 2017, publiait une étude parue dans le journal scientifique turc *Addicta*. Selon cette étude, les adolescents exposés à Internet feraient face à un grand risque de dépendance, laquelle influerait sur leur santé physique et mentale.

> *Young people between the ages of 12 and 18 are considered at-risk for the addiction, while 3.6 percent of adolescents exhibit the risk factors for internet addiction and 21.8 percent of them are on the brink of addiction. The findings indicate that internet usage is becoming very widespread among adolescents and the youth, meaning that the negative effects of technology may increase as internet usage expands more and more among adolescents.* [11]

Mais, malgré ces articles qui démontrent, études à l'appui, les dangers d'une surexposition à Internet pour notre santé, le Web demeure de plus en plus présent dans nos usages quotidiens, et il évolue à un rythme renversant. Ainsi, il est possible aujourd'hui de se connecter à distance de son domicile sur des appareils électroménagers pour préchauffer le four, ou encore de surveiller à distance ce qui se passe dans son appartement grâce à des systèmes de surveillance développés à cet effet.

---

[11] *Daily Sabah,* Health. (2017) *Internet addiction poses grave danger for teens, study reveals.* Récupéré de https://www.dailysabah.com/health/2017/08/10/internet-addiction-poses-grave-danger-for-teens-study-reveals

Ces nouvelles pratiques se sont développées avec l'émergence de l'internet des objets, ce qui va intensifier de manière considérable notre hyperconnectivité. « Now, the Internet edge is pushing towards wireless hyperconnectivity, whereby the density of wirelessly interconnected devices increases dramatically and most devices have multiple wireless interfaces [12] ». Cela peut certes faciliter notre vie quotidienne mais, si nous pouvons nous connecter à distance à ces objets, d'autres peuvent également le faire. Et même si les différentes connexions demeurent sécurisées par des protocoles et des mots de passe que l'on tente de rendre indécryptables, il suffit néanmoins que quelqu'un parvienne à contrer ces systèmes de sécurité pour qu'il pénètre dans nos espaces privés.

1.1.3 Le piratage informatique

Le paragraphe ci-dessous présente la première partie d'un article que l'on a tiré du site internet hackerwifi.net. Il démontre qu'il nous est possible à l'aide d'une simple recherche sur Google – qui dans notre cas nous a orientée vers cette page – de comprendre le fonctionnement élémentaire du piratage internet et de s'y adonner.

> *Pour pirater un réseau WiFi, vous devez d'abord connaître le type de cryptage utilisé. Il existe le cryptage WEP (le plus facile à pirater/cracker), le WPA et le WPA2 et ses variantes. Nous avons développé pour vous un programme au fonctionnement intuitif permettant de détecter le type de cryptage et d'appliquer la méthode de cracking adéquate.*[13]

Nous l'avions évoqué précédemment, Internet prend une place centrale dans nos vies, que ce soit à travers nos interactions sociales ou encore nos usages quotidiens de

---

[12] Peterson, H. Baccelli, E. et Wahlisch, M. (2014). *Interoperable Services on Constrained Devices in the Internet of Things.* Récupéré de https://www.w3.org/2014/02/wot/papers/baccelli.pdf

[13] *hackerwifi.net*

différents objets connectés à des systèmes de contrôle à distance. Chaque nouvelle connexion dans le cyberespace ouvre une porte sur notre vie privée, et la seule protection que nous avons est notre connaissance des meilleures pratiques à adopter lors de notre navigation dans ces réseaux. Mais chaque système a ses failles, et le piratage est une réalité bien présente : de nombreux exemples ont démontré que des pirates ont profité des moindres failles des systèmes de sécurité afin d'attaquer des institutions, des banques, des gouvernements ou encore des individus. Nul n'est donc à l'abri.

1.2 Cybercriminalité et cyberespionnage

La cybercriminalité touche toutes les couches de la société et, la tendance actuelle étant à l'hyperconnectivité, le risque d'en être victime est évident.
Solange Ghernaouti-Hélie, professeure de la faculté des HEC de l'Université de Lausanne et experte internationale en cybersécurité, a souligné dans ses travaux et publications le fait que le développement de la cybercriminalité est intrinsèquement lié au développement d'Internet, et que cela représente un danger majeur pour les usagers, tant les individus que les institutions, les gouvernements, les États.

> *Citoyens détroussés, enfants en danger, entreprises ruinées, États menacés, les cybercriminels étendent leur emprise en même temps qu'Internet se développe. Nous ne les voyons pas, nous ne les connaissons pas, nous ne nous en méfions pas, et c'est leur force. Pourtant, nous sommes tous concernés. Qu'il s'agisse de manipulation d'opinion, d'espionnage, d'usurpation d'identité, de terrorisme, de harcèlement, d'escroquerie, de délinquance, de fraude financière ou de*

> *diverses formes de délinquance, la cybercriminalité touche la société dans son intégralité.*[14]

Les nations sont au cœur de cette cyberguerre qui, selon les auteurs Janczewski et Colarik (2008), est inévitable du fait que le développement technologique rend les nations dépendantes des systèmes informatiques.

> *The more sophisiticated a nation's infrastructures – the more vulnerable it may become. Interdependencies of electrical power grids, accessible computerized systems and other 'softs' targets, alow potential for terrorist intruders* [15]

Selon le chercheur Adam Segal, l'espionnage à l'échelle des nations est devenu pratique courante, notamment pour les grandes puissances telles que les États-Unis. La quête constante d'informations stratégiques étant un enjeu national majeur, cette course effrénée vers la collecte de données permet d'appréhender, mais également de contrer, toute stratégie diplomatique, militaire, ou toute autre offensive de la part d'autres nations qui pourrait nuire à la sécurité, la stabilité ou encore aux intérêts des États. C'est donc une véritable guerre de l'information qui est en cours et, à l'ère de l'information numérique, l'affaire Edward Snowden en est un des exemples les plus probants. Cet ancien employé de la National Security Agency américaine en a révélé les pratiques secrètes, créant un des plus grands scandales du 21^{e} siècle. Ses révélations sur l'espionnage à l'échelle nationale et internationale auquel s'adonnent les agents de la NSA touchent notamment les communications dans le cyberespace; c'est donc également un cas de cyberespionnage avéré.

---

[14] Ghernaouti-Hélie, Solange. (2009) *La cybercriminalité : le visible et l'invisible,* Lausanne : Presses polytechniques et universitaires romandes.

[15] Janczewski, Lech, et M. Colarik, Andrew. (2008). *Cyber Warfare and Cyber Terrorism.* New York : Information Science Reference. Récupéré de http://books.google.com/

> *The president and other policymakers (and their Chinese and Russian counterparts) have become addicted to data and as a result more demanding of their intelligence agencies. Every day the president receives an intelligence briefing, and up to 75 percent of the information contained in the report comes from cyber spies, according to Mike McConnell, director of national intelligence under President George W. Bush. Moreover, the FBI, Department of Homeland Security, and other customers want more access to secret intelligence.*[16]

1.3 Le *hacking*

Avant d'entrer dans le vif du sujet en présentant la série documentaire *Hackers,* il nous semble important de définir le terme « hacker », car il est intrinsèquement relié au contenu de la série. Selon Manuel Castells, professeur de sociologie et titulaire de la chaire du Centre des études sur l'Europe occidentale à l'Université de Californie, à Berkeley, « les *hackers* sont en fait des passionnés d'informatique qui inventent et innovent pour le plaisir, non au service d'une institution ou d'une entreprise[17] ». Pour certains experts, le *hacking* ne serait pas un simple acte isolé, mais il s'organiserait en communauté. « Il existe une communauté – une culture partagée – de programmeurs chevronnés et de sorciers des réseaux dont l'histoire remonte, à travers les décennies, aux premiers mini-ordinateurs multi-utilisateurs et aux premières expériences d'arpanet [18] »

---

[16] Segal, Adam. (2016) *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. New York : Public Affair Tm. Récupéré de http://books.google.com/

[17] Castells, M. (2001) *La Galaxie Internet,* Paris : Fayard.

[18] Raymond, Éric S. (2000) Comment devenir un hacker [chapitre de livre], *dans Olivier BLONDEAU. Libres enfants du savoir numérique* (p. 255-277) Paris: Editions de l'Éclat « Hors collection ».

1.4 La chaîne ICI Explora

La série documentaire *Hackers* est diffusée sur la chaîne spécialisée ICI Explora. Par définition, « une chaîne dite "spécialisée" s'oppose à une chaîne généraliste, qui vise une plus large audience. Une chaîne spécialisée cible ses auditeurs en se focalisant sur une thématique précise[19] ». La chaîne ICI Explora, qui est entrée en ondes en mars 2012, se « consacre aux sciences, à l'environnement et à la santé[20] », selon le Centre d'études sur les médias. La pertinence de ces informations, en ce qui nous concerne, réside dans le fait que cela nous permet de préciser davantage notre objet de recherche : nous ne nous intéressons pas à un média généraliste ou un média de masse avec un fort taux de pénétration.

Nous avons également, dans nos recherches, tenté de déterminer l'auditoire cible de cette chaîne spécialisée, et nous avons pu relever l'information suivante : il serait « masculin, jeune, éduqué et nanti[21] ». Cette donnée supplémentaire nous permet également de souligner que la série documentaire à laquelle nous nous intéressons s'adresse à un auditoire averti, éduqué et intéressé. Notre posture de chercheur nous incline à supposer que cela devrait donc avoir un impact sur le type de contenu et sur les messages portés par cette série en comparaison de ceux que livrerait un média qui cible un public plus large. Nous reviendrons plus en détail sur ce point dans les chapitres suivants, lorsque nous nous intéresserons au cadre théorique et présenterons l'analyse des mécanismes de communication télévisuelle selon le modèle codage/décodage adopté par Stuart Hall.

---

[19] Blogue Lefigaroux. (2009). *Les chaînes spécialisées laissent-elles encore une raison d'exister aux chaînes généralistes ?* Récupéré de *https://lefigaroux.wordpress.com*

[20] Centre d'études sur les médias. (2017) *La télévision.* Récupéré de *http://www.cem.ulaval.ca/pdf/Television.pdf*

[21] Grenier aux Nouvelles. (2015). *ICI Explora : un succès d'abonnement et d'écoute.* Récupéré de *http://www.grenier.qc.ca/nouvelles/8598/ici-explora-un-succes-dabonnement-et-decoute*

1.5 La série documentaire *Hackers*

La série documentaire *Hackers* a été produite et diffusée en 2016 sur les ondes d'ICI Explora, chaîne du diffuseur Radio-Canada. Elle tente de vulgariser la cybercriminalité et de mettre en lumière les limites de la protection des données personnelles dans l'utilisation d'Internet et notamment dans les réseaux sociaux. Elle met notamment l'accent sur certaines formes de cybercriminalité (vol d'identité, cyberintimidation, fraude) tout en démontrant les failles dans les pratiques des consommateurs, qui permettent aux *hackers* de commettre leurs crimes.

> *Montréal, le 19 octobre 2016 – Dès le vendredi 28 octobre, à 19 h 30, sur les ondes d'ICI EXPLORA, accompagnez Matthieu Dugal à la rencontre des « hackers », ces génies de l'informatique qui œuvrent dans l'ombre pour défier la loi et profitent des failles de sécurité informatique pour mener à bien leurs plans. Une occasion d'en apprendre plus sur eux, qui en savent tant sur nous!*[22]

Cette série documentaire souligne notamment le fait que la cybercriminalité ne cible pas uniquement les grandes institutions telles que les banques ou les gouvernements, mais qu'elle touche également les individus alors que ces derniers pensent souvent être à l'abri des *hackers*. Sur le plan de la communication, cette série met l'accent sur l'émergence d'une nouvelle forme d'interaction sociale, qui s'exerce à travers les identités numériques. Finalement elle est également elle-même un média de communication et livre de nombreux messages à l'intention des téléspectateurs.

Cette série documentaire se propose donc de décrypter le vaste monde de la cybercriminalité de manière ludique et éducative, en cinq chapitres qui couvrent

---

[22] Radio-Canada. (2016). *La série HACKERS lève le voile sur le monde obscur des pirates informatiques*. Récupéré de *http://servicesfrancais.radio-canada.ca*

différentes thématiques. La vulgarisation de l'information se fait à travers des exemples concrets de cybercriminalité, décryptés et analysés par des experts.

1.6 Question centrale et hypothèse d'ensemble

À la lumière de ce que nous venons de voir, il apparaît clair que notre recherche porte à la fois sur les communications, le cyberespace et la cybercriminalité. Dans un monde en constante évolution numérique, nous nous intéressons à la mise en lumière de certaines problématiques liées à la protection des données et à la cybercriminalité sous ses diverses formes. Ces problématiques nous poussent à nous questionner sur le degré de connaissance, de la part des usagers, des risques auxquels ils s'exposent dans le cyberespace, mais également sur les canaux de communication mis en place afin de les y sensibiliser. Comme nous l'avons mentionné en introduction, les politiques gouvernementales s'inscrivent dans une logique de sensibilisation à l'importance d'Internet comme accélérateur de croissance socioéconomique du pays. Mais nous nous questionnons sur la protection des données personnelles et sur les comportements à risque dans le cyberespace. À l'heure du *big data*, une quantité importante d'informations circule sur Internet, et ces informations, lorsqu'elles tombent dans les mains de *hackers,* peuvent nuire à ceux qu'elles concernent. Voilà pourquoi nous nous sommes particulièrement intéressés à la série documentaire *Hackers :* d'une part, en sa qualité de média, elle se présente naturellement comme objet de recherche en communication; et, d'autre part, son contenu visant manifestement à sensibiliser, informer et éduquer sur les enjeux liés à la cybercriminalité, cette série répond doublement à l'intérêt de notre recherche. Nous posons donc la question centrale suivante : comment la série documentaire *Hackers* communique, sensibilise et éduque sur les grands enjeux liés aux identités numériques et à la cybercriminalité?

1.6.1 Questions sectorielles

Différentes questions sectorielles viennent alimenter notre analyse. Ces questions permettent également de baliser notre recherche, car elles constituent des axes de réflexion qui structurent notre démarche méthodologique.
Nous avons pleinement conscience de l'importance d'Internet, et l'avons intégré dans nos usages quotidiens. Nos gouvernements mettent aujourd'hui en place des politiques visant à faciliter son accessibilité à un maximum de personnes. Dans ce contexte, les questions suivantes se posent naturellement :

- Qu'en est-il des enjeux de cybersécurité inévitablement reliés à l'utilisation de la communication en ligne ?
- Quelles sont nos connaissances des risques liés à l'utilisation d'Internet ?
- Nos identités numériques sont-elles protégées dans le cyberespace ?
- Nos habitudes de consommation sont-elles sécuritaires ?
- Avons-nous conscience des brèches du système, et des dangers auxquels nous sommes exposés dans le cyberespace ?
- Quel est le rôle que peut jouer la série *Hackers* et quels sont les principaux messages qu'elle véhicule ?
- Quel est l'objectif communicationnel du réalisateur et comment construit-il son message?
- Les objectifs du réalisateur sont-ils atteints auprès de l'audience?
- Les messages clés construits dans le scénario de la série par le réalisateur ont-ils été perçus de la même manière par l'audience ?

- Est-ce que le degré de compréhension des messages diffère d'une audience à une autre ?
- Est-ce que l'audience accepte d'emblée les messages de la série ou a-t-elle tendance à manifester une certaine résistance ?

1.6.2 Pertinence communicationnelle

À notre avis, ce mémoire s'inscrit parfaitement dans les champs de recherche qui concernent les communications. En effet, il a pour objectif premier de mettre en lumière la pertinence de la diffusion de l'information à travers les canaux médiatiques. Il s'intéresse également à la perception des messages et à leur impact sur le comportement des consommateurs qui les reçoivent. Ce mémoire soulève entre autres des problématiques propres aux communications numériques et à nos interactions dans le cyberespace. Du fait qu'Internet comme mode de communication est largement répondu et que le cyberespace est le lieu de socialisation contemporain par excellence, il devient primordial pour tout chercheur qui s'intéresse aux enjeux de communication de comprendre ces phénomènes d'interactions sociales, leur systèmes de déploiement et d'en saisir les mécanismes. L'analyse des communications dans un objectif de sensibilisation aux problématiques liées à la cybercriminalité constitue le cœur de ce mémoire. La série *Hackers* étant diffusée par un média spécialisé, elle nous offre un cadre propice à analyser et comprendre le processus de production de messages dans un contexte donné, mais également tout désigné pour évaluer la réception de ce message en sondant l'auditoire auquel il est destiné.

CHAPITRE II

DÉLIMITATION DU CADRE THÉORIQUE

Dans ce chapitre, nous décrirons les théories qui nous ont servi de cadre d'analyse. Ce mémoire s'inscrit dans le champ des communications, et plus précisément dans ce qui a trait à la communication médiatique, mais il a également un point d'ancrage dans les interactions sociales et comportementales avec le cyberespace. Il s'intéresse également au *hacking*, qui est un phénomène intrinsèquement relié au cyberespace. À la lumière de ces grands axes de réflexion, nous fonderons notre cadre de référence théorique sur trois grands ouvrages qui baliseront notre analyse.

2.1 *Cyberespace et communautique,* de Pierre-Léonard Harvey

L'ouvrage de Pierre-Léonard Harvey constitue pour nous une référence théorique des plus pertinentes. En effet, le chercheur met en lumière dans son ouvrage un principe clé en lien avec notre objet de recherche, à savoir « l'appropriation sociale des objets techniques de communication[23] ». Notre navigation dans le cyberespace se faisant au travers d'objets techniques de communication, les travaux de Pierre-Léonard Harvey

---

[23] Harvey, Pierre-Léonard. (1995). *Cyberespace et communautique,* Québec : Presses de l'Université Laval. Récupéré de *https://books.google.ca*

nous aident à mieux encadrer notre analyse du comportement des usagers et de leur appropriation du cyberespace.

> *Pierre-Léonard Harvey examine tour à tour le développement et le mode d'insertion sociale des nouvelles techniques d'information et de communication (NTIC). Il soutient que leur adoption dépend moins de leur mode de diffusion et de leurs caractéristiques fonctionnelles ou techniques que de la façon dont les gens réinventent et s'approprient ces techniques.*[24]

Il pose non seulement les principes théoriques fondamentaux du comportement humain dans le cyberespace, mais il met également en lumière les différentes interactions qui se créent dans le cyberespace dans une analyse multidisciplinaire de ces interactions. En effet, l'auteur se réfère à la fois à des notions théoriques émergentes de la psychosociologie, de l'économie ou encore de la sociologie. Par son travail, le chercheur démontre la complexité de la construction des interactions qui coexistent dans le cyberespace. Dans le cadre de notre travail de recherche, il nous permet donc de baliser notre démarche en approfondissant notre compréhension de ces échanges qui se créent dans le cyberespace.

> *Il met en évidence la permanence des structures sociales tout en montrant de quelle manière l'opulence communicationnelle créée par les inforoutes est susceptible de modifier les échanges à l'intérieur des communautés existantes.* [25]

Pierre-Léonard Harvey aborde également la notion de *communautique,* qu'il définit comme « un espace public caractérisé par une communication entre groupes, c'est-à-dire entre les membres et leur groupe, entre les membres eux-mêmes et entre les

---

[24] *Ibid.*
[25] *Ibid.*

groupes eux-mêmes ». « Ces groupes possèdent des intérêts communs »[26], ajoute-t-il. Dans un travail de recherche s'inscrivant dans le champ des communications et traitant du cyberespace comme lieu d'échanges, la compréhension des caractéristiques inhérentes aux groupes qui y interagissent nous permet de mieux baliser notre recherche, tout en étayant notre analyse de références théoriques pertinentes.

2.2 Stuart Hall : codage et décodage

Si les travaux de Pierre Léonard Harvey nous permettent de mieux comprendre le comportement social des internautes dans le cyberespace, nous avons fait appel, dans un souci de compléter nos références théoriques mais surtout d'approfondir notre analyse, à un autre auteur de référence.

Le choix de Stuart Hall s'est imposé à nous alors que nous tentions de comprendre comment les messages se construisent et se transmettent à travers un « produit médiatique » et comment évaluer la réception de l'auditoire.

En effet, si nous nous sommes intéressées aux messages clés portés par la série, nous avons porté également de l'intérêt au type de réception de ces messages par l'auditoire. C'est donc à ce moment que le processus de communication télévisuel auquel s'est intéressé Stuart Hall est devenu un élément central de notre recherche. Et, même si ses travaux ciblent majoritairement les médias de masse, ils demeurent néanmoins pertinents pour notre recherche, car ils nous permettent de baliser l'analyse des « messages médiatiques » selon une approche « non linéaire » et en considérant que le récepteur est aussi un participant « actif ».

---

[26] *Ibid.*

2.2.1 Du « schéma de Laswell » à la « réception active » de Hall

Rappelons que les approches en communication médiatique ont beaucoup évolué. En effet, les approches classiques considéraient la communication médiatique comme un processus linéaire, et n'accordaient pas d'importance ou de rôle particulier au récepteur. Mais, dans les approches plus contemporaines, le public (récepteur) est devenu un élément central du processus de communication. Notre but ici n'est pas de retracer l'historique des approches utilisées ou des théories portant sur les communications médiatiques, mais il nous apparaît important de souligner l'évolution de ces dernières, car cela permet de rappeler que la recherche en communication demeure en constante évolution. Cela nous permet également de souligner l'apport de Stuart Hall dans cette évolution, et de justifier notre choix en mettant de l'avant ses concepts clés, et en les appliquant à notre objet de recherche.

Dans l'étude de la communication, Stuart Hall a apporté un changement majeur en introduisant l'approche de la « réception active », alors que des chercheurs comme Laswell considéraient que les médias avaient un pouvoir de contrôle et de persuasion total sur le public (non actif). Avant Hall, on avait plutôt l'habitude, chez Bryson par exemple, de constater « les effets directs et puissants des médias sur l'isolement social du public », les médias utilisant des moyens psychologiques pour persuader « une masse aliénée, tétanisée et amorphe [27] ».

Le processus de communication ou « schéma de Laswell [28] » impliquait donc un public (récepteur) non « actif », qui absorbait l'information telle qu'elle était présentée, sans la remettre en question. D'où la célèbre expression de la « seringue hypodermique [29]. »

---

[27] Bryson, Lyman (1948). *The Communication of Ideas,* New York : The Institute for Religious and Social Studies.

[28] *Ibid.*

[29] Cette expression (« hypodermic needle ») rend compte de l'influence des médias sur la « masse ». Cf. lasswell, Harold. (1927). *Propaganda Techniques in the World War I,* New York: Knopf. Récupéré de http://www.mei-info.com/wp-content/uploads/revue24-25/20MEI-24-25.pdf

Stuart Hall a, quant à lui, repositionné le récepteur dans le processus de communication médiatique, considérant le fait que les médias produisent des discours, mais qu'« une fois achevé, le discours doit donc être traduit – transformé de nouveau – en pratiques sociales si l'on veut que le circuit soit complet et efficace[30] ».
Le chercheur a fait du public un élément central du processus de communication médiatique, en considérant que c'est à lui qu'il revient « d'extraire » le discours et de le « traduire » pour lui donner un sens. « Si aucun "sens" n'est extrait, il ne peut y avoir de "consommation" [31] ». Stuart va plus loin dans ses recherches en s'intéressant davantage au public qui « consomme » le produit médiatique. Il va ainsi lui attribuer un rôle de « récepteur actif » et classifier, dans son analyse du processus de la communication, les différents types de réception que peut avoir le public.

2.2.2 L'approche codage/décodage

Stuart va donc développer une approche qui nous permet de comprendre comment se construit un message médiatique. Pour cela, il va considérer que le processus de communication a ses propres « déterminants », et se compose de « moments ». Selon lui, « dans un moment "déterminé", la structure emploie un code et génère un "message" ; à un autre moment déterminé, le "message", par l'intermédiaire de ses décodages, débouche sur la structure des pratiques sociales[32] ».
Le message médiatique passerait donc par deux étapes majeures :

---

[30] Hall, Stuart. CCCS, Albaret, Michèle. et Gamberini, Marie-Christine. (1994) *« Codage/décodage »*, [chapitre de livre] In: *Réseaux,* volume 12, n° 68, 1994. *Les théories de la réception.* (p. 27-39). Récupéré de *www.persee.fr/doc/reso_0751-7971_1994_num_12_68_2618*
[31] *Ibid.*
[32] *Ibid.*

– le codage (la composition originelle du message)[33];
– le décodage (moment où le message est « lu » et « compris »)[34].

Si nous appliquons cette approche à notre objet de recherche qui est la série *Hackers,* nous pouvons considérer que le codage prend forme au moment où le réalisateur construit son scénario afin de transmettre ses messages. Quant au décodage, il se produit lorsque l'auditoire, visionnant la série, tente d'en extraire ces dits messages pour leur donner un sens et ainsi « consommer » le produit médiatique.

2.2.3 Les trois positions « hypothétiques » de réception des messages médiatiques

Comme nous l'avons vu, Stuart Hall accorde un rôle déterminant au récepteur dans le processus de diffusion d'un message médiatique. En s'intéressant à ses travaux, on peut ainsi lire ce qui suit :

> *Les processus classiquement identifiés par la recherche positiviste sur des éléments isolés – effets, usages, « gratifications » – sont eux-mêmes façonnés par des structures de compréhension, tout en étant produits par des rapports sociaux et économiques qui façonnent leur « réalisation » à l'autre bout de la chaîne – celui de la réception – et permettent aux sens signifiés dans le discours d'être transposés dans la pratique ou la conscience (pour acquérir une valeur d'usage social ou une efficacité politique).* [35]

Ce que Stuart Hall nous démontre, c'est que les processus de codage et d'encodage sont influencés autant par l'émetteur du message que par son récepteur : du fait qu'ils évoluent dans des environnements et des cultures propres, ils sont influencés par ces

---

[33] *Ccnpps.ca* (2010) *Comprendre les communications médiatiques. L'approche encodage/décodage.* Récupéré de *http://www.ccnpps.ca/docs/2010_ProcessusPP_SI2010_ComprendreComMedia_Fr.pdf*
[34] *Ibid*
[35] *Op. cit.*

derniers, et cela aura une incidence au moment du décodage. Donc, si on poursuit dans cette logique, on peut postuler qu'un message est forcément codé de manière différente par différents émetteurs, mais surtout qu'il est décodé de manière différente par différents récepteurs. C'est ici que se pose la question de déterminer quel type de réception aura, d'un message particulier, un auditoire cible. Stuart Hall s'est intéressé à cette question dans ses travaux et il en est venu à la conclusion que les « degrés de "compréhension" et de "méprise" dans l'échange communicationnel dépendent des degrés de symétrie/asymétrie (relations d'équivalence) entre les positions des "personnifications" du codeur-producteur et du décodeur-récepteur[36] ».

Ainsi, on construirait un message selon la culture et l'environnement dans lequel on évolue, et on le décoderait également selon ces mêmes paramètres. Et si ces derniers changent, il peut y avoir une distorsion dans la compréhension du message. Cela prend tout son sens lorsque l'on pense aux différentes perceptions relatives à un film, une série ou même un documentaire par des publics évoluant dans des environnements et des cultures différents. Cela explique également le succès ou la déconvenue de certaines productions médiatiques selon le pays de diffusion. À ce sujet, Hall explique ce qui suit :

> *Le plus souvent, les producteurs d'émissions déplorent que le public n'ait pas saisi le sens qu'eux-mêmes cherchaient à faire passer. Or ce qu'ils veulent dire, en réalité, c'est que les téléspectateurs ne fonctionnent pas au sein du code « dominant » ou « préféré ». Les diffuseurs ont un idéal de « communication parfaitement transparente » et, à la place, il leur faut faire face à une « communication systématiquement déformée ».* [37]

Hall a même tenté d'analyser les différents types de réception que l'on peut avoir en déterminant trois positions « hypothétiques » à partir desquelles les textes médiatiques peuvent être compris.

---

[36] *Ibid.*
[37] *Ibid.*

a) La position dominante-hégémonique

On considère qu'il y'a une position dominante-hégémonique lorsque le message médiatique est perçu par le public tel qu'il avait été conçu par son producteur. Ainsi, pour Hall, il y aurait dans ce cas une communication « parfaitement transparente ». Et, pour lui, cela impliquerait ce qui suit :

> *Un spectateur intègre directement et sans restrictions le sens connoté d'informations télévisées ou d'une émission d'actualités, par exemple, et décode le message en fonction du code de référence qui a servi à le coder. On pourrait dire que ce téléspectateur opère au sein du code dominant.* [38]

Le public ne présenterait ici aucune forme de résistance et adhérerait aux valeurs et contenus des messages sans aucune distorsion de « sens ».

b) La position négociée

Cela s'appliquerait aux cas où il y aurait une légère distorsion entre le message produit et le message perçu. Hall définit cette position ainsi :

> *Le décodage au sein de la version négociée renferme un mélange d'éléments adaptatifs et oppositionnels : il reconnaît la légitimité des définitions hégémoniques pour établir (dans l'abstrait) les grandes significations, tandis qu'à un niveau plus limité, situationnel (situé), il pose ses propres règles de base.*[39]

On comprend ici que le message demeure dans ce cas perçu par le récepteur, mais qu'il y oppose une certaine résistance en raison de ses propres connaissances. Ainsi, il

---

[38] *Ibid*
[39] *Ibid*

filtre ce qu'il perçoit, selon son propre cadre de référence. Selon Hall, dans ce cas, « les codes négociés fonctionnent à travers ce que l'on pourrait appeler des logiques situées, ou particulières. Et ces logiques sont entretenues par leurs relations inégales et différentielles avec les discours et logiques du pouvoir [40] ».

c) La position oppositionnelle

Si, dans la position précédente, il y avait une compréhension du message avec néanmoins une certaine distorsion, dans ce cas, le récepteur manifeste une résistance totale au message. Pour Hall, cela implique ce qui suit :

> *Il est possible qu'un téléspectateur comprenne parfaitement toutes les inflexions littérales et connotatives fournies par un discours, mais décode le message de manière globalement contraire. Il détotalise le message dans le code préféré pour le retotaliser dans un autre cadre de référence.*[41]

Les travaux de Stuart Hall nous offrent un cadre de référence théorique solide mais surtout concordant avec notre objet de recherche, et nous nous en servirons dans notre analyse du processus de communication dans la série documentaire *Hackers.*

2.3 *The Hacked World Order,* d'Adam Segal

Nous avions aussi besoin de faire appel à un auteur de référence en ce qui concerne les questions relatives à la cybercriminalité. À cet égard, le chercheur Adam Segal apparaît comme un auteur de référence clé, du fait que son ouvrage couvre l'ensemble des problématiques soulevées dans notre travail de recherche. Dans son ouvrage *The Hacked World Order : How Nations Fight, Trade, Maneuver, and*

---

[40] *Ibid*
[41] *Ibid*

Manipulate in the Digital Age, il démontre bien les comportements à risques au sein du cyberespace et le rôle du piratage dans l'espionnage, la cyberdiplomatie et le cyberterrorisme. Notons quelques sujets qu'il aborde :

- Everyone is Spying (la montée de l'espionnage);
- Stuxnet Case Study (le cas du virus Stuxnet [Israël–États-Unis]);
- The United States is a Very Active Participant in Worldwide Surveillance (le programme NSA des États-Unis et l'affaire Snowden);
- Hacking as a National Security Threat (le *hacking* comme menace pour la sécurité nationale);
- Hacking as a New Form of Corporate Espionage (le *hacking,* nouvelle forme d'espionnage industriel);
- Propaganda in the Age of Twitter (la propagande à travers les médias sociaux – le cas de Twitter);
- Détente in Cyberspace? (cyberdiplomatie, négociations et ententes bilatérales).

Ces différentes problématiques concordent avec celles abordées dans la série documentaire *Hackers*. Ainsi, Adam Segal nous offre un cadre de référence théorique contemporain afin de structurer notre analyse. La cybercriminalité étant elle-même un phénomène émergent, les travaux de Segal ont constitué pour nous une référence très utile, car ils nous ont permis de mieux comprendre ce phénomène relativement nouveau.

2.4 Synthèse et lien avec notre objet de recherche

Il est important de rappeler ici que notre travail de recherche touche deux formes de communication médiatique. Notre mémoire porte d'abord sur la série documentaire *Hackers,* mais le choix de cette série est dû au fait que nous nous intéressons également à la cybercriminalité. Cette dernière est une réalité qui prend de plus en plus d'ampleur au sein du cyberespace, haut lieu de nos interactions contemporaines. La série documentaire télévisée est une forme médiatique plutôt traditionnelle, alors que la cybercriminalité est un phénomène intrinsèquement lié au cyberespace, considéré comme une forme de communication médiatique tout à fait contemporaine. Pour observer ces sujets, nous avons mis l'accent sur trois grands auteurs qui, par leurs travaux, nous offrent des éléments de référence théoriques pertinents qui nous permettent d'analyser de manière cohérente ces différentes formes de communication, l'une traditionnelle et l'autre essentiellement contemporaine. Même si l'intérêt au sujet du comportement et des modes de communication dans le cyberespace demeure encore très récent, les travaux de Pierre-Léonard Harvey nous permettent de conceptualiser ces comportements tout en développant une terminologie qui leur est propre. Harvey souligne à ce sujet ce qui suit :

> *Dans le contexte actuel des médias interactifs, contrairement au contexte mass médiatique, lorsque les habitudes d'utilisation s'installent, nous ne parlons plus de public ou de téléspectateurs mais bien d'usagers. Cette terminologie est importante, car les contextes de consommation des médias se sont passablement modifiés : d'une situation de diffusion et d'influence linéaire, les médias sont passés à des contextes d'échange, grâce à l'interactivité des outils.*[42]

---

[42] Harvey, Pierre-Léonard. (1995). *Cyberespace et communautique,* Québec : Presses de l'Université Laval. Récupéré de https://books.google.ca

Nous pensons que ses travaux peuvent servir de base à toute recherche portant sur le cyberespace, car il effectue une analyse multidisciplinaire des comportements et des modes d'interactions qui lui sont propres. Il nous permet également de mieux comprendre comment nous nous approprions les objets modernes de communication, en analysant les différentes dimensions de cette appropriation, qu'elles soient culturelle, juridique, géographique, spatial, organisationnelle, anthropologique, économique ou encore politique. Et il met en lumière la complexité de cette appartenance en soulignant que l'« on aurait tort de croire que *virtuel* signifie simplement accès à des contenus extraterritoriaux et non pas des possibilités d'appartenance réelle à des communautiques d'intérêt [43] ».

Nous considérons donc que l'apport de Harvey est essentiel à notre recherche, car la lecture de ses travaux nous permet de conforter notre choix d'inscrire notre intérêt pour les enjeux relatifs au cyberespace dans le champ de l'analyse des communications.

Nous avons de même trouvé dans l'approche *codage/décodage* de Stuart Hall une référence majeure pour définir notre méthodologie, car cette approche nous permet non seulement de comprendre comment se construit un message médiatique, mais aussi de catégoriser les types de réception que l'on peut avoir de ce message. Même si Hall s'intéressait à des médias de masse – dont *Hackers* ne fait pas partie – son analyse nous a paru tout à fait pertinente pour analyser d'une part le message véhiculé par le réalisateur et, d'autre part, les messages perçus par les téléspectateurs de la série. L'objectif de notre recherche est ainsi d'analyser, en ayant recours aux concepts de Hall, les degrés de « compréhension » **et** de « méprise » (la « symétrie/asymétrie ») entre les deux « acteurs » de la série : le réalisateur et les téléspectateurs.

---

[43] *Ibid.*

Le travail de P.-L. Harvey nous a donc aidées à comprendre le comportement des usagers dans le cyberespace, et celui de S. Hall à comprendre le processus de communication télévisuel et les types de réception qui en découlent.

En plus de ces deux auteurs, nous avons eu recours au travail d'Adam Segal pour nous éclairer en ce qui concerne les questions de cybercriminalité. En effet, dans son livre *The Hacked World Order*, Segal a analysé de manière approfondie les différentes formes de cybercriminalité, un sujet qui est au centre même de la série *Hackers.*

> *The conflict in cyberspace will only become more belligerent, the stakes more consequential. An estimated 75 percent of the world's population has now access to a mobile phone, and the Internet connects 40 percent of the planet's population, roughly 2, 7 billion people. Information and communications networks are embedded in our political, economic and social lives. Individuals and civil society now participate in global politics in new ways but sovereign states can do astonishing and terrifying things that no collection of citizens or subjects can carry out. We will be caught in the fallout as the great powers, and many of the lesser ones, attack, surveil, influence, steal from, and trade with each other.*[44]

Segal constitue une référence de premier plan en ce qui concerne le sujet central de *Hackers,* et c'est la raison pour laquelle nous avons eu recours à son travail. « Segal examines numerous instances of cyberwar, some of which may come as news to readers…Netizens and white-hat programmers will be familiar with Segal's arguments, but most policymakers will not—and they deserve wide discussion[45] ».

---

[44] Segal, Adam. (2016) *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age,* New York : Public Affair Tm. Tiré de http://books.google.com/

[45] Publicaffairsbooks.com (s. d.). Récupéré de http://www.publicaffairsbooks.com/book/the-hacked-world-order/

CHAPITRE III

PRÉSENTATION DE LA MÉTHODOLOGIE

Nous avons adopté dans ce travail de recherche une approche qualitative, qui permet de mieux saisir les phénomènes communicationnels en lien avec notre objet de recherche. Nous allons donc dans ce chapitre présenter notre démarche, utilisée pour analyser la série *Hackers* mais également pour analyser les messages qu'elle veut véhiculer et leur réception par l'audience.

3.1 Pertinence de l'approche qualitative et démarche de recherche

Afin de répondre à notre question de recherche, à savoir *Comment la série documentaire* Hackers *communique, sensibilise et éduque sur les grands enjeux liés aux identités numériques et à la cybercriminalité?,* nous avons choisi de réaliser une étude de réception de nature qualitative.

Dans le cadre de notre travail, nous ne nous intéressons pas aux données de type statistique mais plutôt aux expériences personnelles de réception de la série par l'auditoire, grâce à des entrevues que nous avons réalisées avec des téléspectateurs de la série.

Notre but n'est donc pas d'avoir une vision quantitative des informations collectées, mais plutôt de faire une analyse qualitative de ces dernières. Voici pourquoi l'approche qualitative nous est apparue plus pertinente.

> *La recherche qualitative se caractérise par une approche qui vise à décrire et à analyser la culture et le comportement des humains et de leurs groupes du point de vue de ceux qui sont étudiés. Par conséquent, elle insiste sur la connaissance complète ou « holistique » du contexte social dans lequel est réalisée la recherche. La vie sociale est vue comme une série d'événements liés entre eux, devant être entièrement décrits, afin de refléter la réalité de la vie de tous les jours. La recherche qualitative repose sur une stratégie de recherche souple et interactive.*[46]

Les entrevues semi-dirigées que nous avons réalisées sont constituées d'échanges autour de questions qui découlent de notre problématique et ont été centrées sur des questions connexes. Notre méthodologie s'inspire des travaux de David Morley[47], qui souligna en 1993 que les médias devaient être considérés comme une construction faite par leur public : « La polysémie du message n'exclut pas qu'il obéisse à une structure. Les publics ne voient pas simplement dans un texte ce qu'ils veulent y voir, dès lors il ne s'agit pas d'une fenêtre ouverte sur le monde, mais d'une construction[48] ».

Ainsi, les analyses de Morley l'ont amené à observer la télévision en tant que technologie domestique intégrée dans une dynamique familiale. L'objectif de ses

---

[46] Rocare. *(s. d.) Extrait de guides pour la recherche qualitative.* Récupéré de *http://www.ernwaca.org/panaf/RQ/fr/definition.php*

[47] Morley, David. (1992) *Television, Audiences and Cultural Studies,* Londres: Routledge

[48] Morley, D. et Dayan, D. *(1993) La réception des travaux sur la réception. Retour sur* « Le public de Nationwide », *Hermès, La Revue* 1993/1 (n° 11-12), p. 31-46. Récupéré de *https://www.cairn.info/load_pdf.php?ID_ARTICLE=HERM_011_0031*

recherches était de « prendre en compte l'épaisseur des interactions dans les consommations médiatiques ».[49]

Aux fins de notre recherche, nous avons choisi de constituer un échantillon du public en regroupant différents profils de consommateurs d'Internet. Dans le but que cet échantillon soit représentatif, nous avons veillé à choisir différents profils de personnes, de façon à reconstituer une microsociété composée de groupes d'âge, de sexe, mais également de niveau d'instruction variés. Nous pensons que ce choix est pertinent, car notre série s'adresse à des personnes ayant avant tout un intérêt pour Internet. De plus, en choisissant des profils de consommateurs différents, nous pouvons ainsi analyser leur réceptivité au sujet de la cybercriminalité dans un cadre de référence propre à leurs différents usages et modes de consommation d'Internet.

La recherche qualitative cadre parfaitement avec notre objet, mais également notre champ de recherche, car elle nous offre la possibilité d'analyser et comprendre les données collectées à travers les entrevues réalisées avec le réalisateur, mais également avec différents membres de notre échantillon.

> *La recherche qualitative est un ensemble de techniques d'investigation dont l'usage est très répandu. Elle donne un aperçu du comportement et des perceptions des gens et permet d'étudier leurs opinions sur un sujet particulier, de façon plus approfondie que dans un sondage. Elle génère des idées et des hypothèses pouvant contribuer à comprendre comment une question est perçue par la population cible et permet de définir ou cerner les options liées à cette question. Cette technique sert beaucoup au prétest des concepts*[50]

Après avoir sélectionné les membres – diversifiés – de notre échantillon, nous leur avons fait visionner cinq épisodes de la série documentaire *Hackers,* en vue

---

[49] Mattelart, A. et Neveu, É. (1996). Cultural studies stories : La domestication d'une pensée sauvage? *Réseaux,* n° 20. p. 29. Récupéré de *http://www.enssib.fr/autres-sites/reseaux-cnet/80/01-matte.pdf*

[50] *Op. cit.*

d'analyser leurs perceptions des messages véhiculés dans lesdits épisodes. Et, en premier lieu, nous avons effectué une entrevue avec le réalisateur de la série.

Il faut ici rappeler que nous avons choisi de prendre pour référence théorique le processus *codage/décodage* développé par Stuart Hall : il nous fallait donc procéder en deux étapes. Comme l'explique Serge Proulx, l'étude de la réception a pour objet l'analyse de « l'interaction qui existe entre les contenus médiatiques et les lectures qui en sont faites par leurs usagers », cette analyse se faisant sur trois plans : « sémiotique, conversationnel et ethnosociologique » (Proulx, 1998, p. 125). Ainsi, la première partie de notre démarche a consisté à déterminer les objectifs communicationnels du réalisateur ainsi que les messages clés véhiculés par le scénario.

En deuxième étape, nous avons constitué notre échantillon et réalisé des entrevues semi-dirigées afin d'analyser les diverses réceptions de la série à partir des données collectées au cours des deux étapes.

3.2 Choix des participants

Comme nous voulions rendre notre échantillon représentatif de la variété des usagers d'Internet, nous avons d'abord dressé une liste des différents profils qu'il nous semblait devoir y retrouver.

Profil 1) L'étudiant(e) universitaire :

Utilise fréquemment Internet, notamment pour ses recherches académiques, a un compte sur les réseaux sociaux et utilise différents services sur Internet, par exemple des services bancaires en ligne. Il ou elle se connecte souvent à des réseaux publics, par exemple dans des cafés, afin de profiter d'une connexion à moindre coût.

Profil 2) L'aîné(e) :

Est à la retraite, et a donc du temps libre. Il ou elle dispose d'une connexion Internet et l'utilise pour garder contact avec ses petits-enfants ou ses enfants qui vivent à distance. Il ou elle utilise Internet de manière peu fréquente, mais a accès à certains services via le Net.

Profil 3) La mère de famille :

Elle utilise Internet assez fréquemment, et est très occupée. Elle considère Internet comme une source d'informations pratiques. Elle a des enfants qui se connectent et elle s'intéresse de près à leur usage d'Internet.

Profil 4) Le/La jeune professionnel(le) :

Éduquée et professionnellement établie, cette personne utilise Internet de manière très fréquente. Elle suit l'actualité et est au fait de nombreuses nouvelles concernant le monde ou la société.

Profil 5) Le/La *geek* :

Cette personne a une connaissance avancée d'Internet, utilise très fréquemment son ordinateur et différents outils technologiques. Elle est connectée à différentes applications, et est au fait des plus récentes tendances. Elle a des notions ou des connaissances approfondies dans le domaine du *hacking*.

Profil 6) L'adolescente :

Elle vit dans un univers hyperconnecté, possède un compte dans pratiquement l'ensemble des réseaux sociaux (Facebook, Snapshat, Instagram). Elle utilise Internet de manière très fréquente. Elle prend souvent des *selfies*. En résumé, elle accorde une grande importance à son identité virtuelle.

Profil 7) L'anarchiste antitechnologie :[51]
Se considère comme une personne qui vit en marge de la société, et limite donc ses interactions sociales. Il ou elle revendique la non-utilisation de la technologie et le retour à des interactions « humaines » plutôt que virtuelles.

3.3 Nature des données

La première partie des données recueillies a été constituée lors de l'entrevue effectuée avec le réalisateur de la série. Cette entrevue nécessitait d'établir au préalable des questions pertinentes. En effet, selon Hall, s'intéresser au décodage d'un texte suppose d'étudier la réception de celui-ci, mais tout en ayant réalisé « une analyse préalable des structures du texte médiatique » (Proulx, 1998, p. 128).
À cette fin, nous avons effectué plusieurs visionnements de la série documentaire afin de déterminer précisément les thématiques qui y sont abordées. Cette étape s'est étalée sur une période de trois semaines, par une moyenne de trois visionnages par épisode, soit environ 450 minutes, en considérant qu'un épisode dure 30 minutes. Il était très important pour nous en effet, de ne pas faire une lecture superficielle de la série, mais de bien comprendre les sujets abordés afin d'être à même de mener les différentes entrevues.
Les informations recueillies nous ont servi à rédiger notre questionnaire, et ont également servi de balises à l'entrevue semi-dirigée que nous avons menée avec le réalisateur.
L'entrevue semi-dirigée avec le réalisateur s'est étalée sur une durée de 1 h 30, et les données recueillies lors de cette entrevue ont été catégorisées en cinq grandes thématiques, telles qu'abordées dans les cinq épisodes de la série. La seconde partie

---

[51] *Voir section 3.5 Composition de l'échantillon, où nous expliquons les raisons pour lesquelles nous avons modifié ce profil.*

des données recueillies sont tirées des sept entrevues individuelles semi-dirigées réalisées avec les participants sélectionnés. Ces entrevues ont été d'une durée de 40 à 60 minutes. Le questionnaire soumis aux répondants a été modulé au cours des différentes entrevues, et ce, en fonction des réponses obtenues. Les résultats de ces entrevues ont été également catégorisés suivant les thématiques abordées par la série.

3.4 Collecte des données

L'entrevue avec le réalisateur de la série, Bachir Bensaddek, s'est déroulée dans un contexte ouvert et dynamique, car nous lui avions exprimé notre intérêt pour sa série et expliqué l'objectif de notre recherche. Il nous avait d'ailleurs donné libre accès au visionnage des épisodes. Nos questions permettaient de couvrir les différents épisodes et avaient pour but de bien cerner les messages clés de la série.

La seconde phase des entrevues s'est déroulée avec les participants sélectionnés pour la recherche. Sur les sept entrevues, une seule a dû être réalisée à l'aide du logiciel de vidéoconférence Skype, les autres s'étant effectuées en personne.

Lors du dépôt du projet de mémoire, nous avons évoqué la possibilité de conduire des entrevues de groupe, mais nous avons décidé finalement d'effectuer des entrevues individuelles, de façon à éviter toute interférence entre les participants.

Ces entrevues individuelles se justifiaient aussi par une réflexion de David Morley, qui a inspiré notre méthodologie. En effet, aux fins de ses études ethnographiques, il préconisait de rencontrer ses participants dans le milieu qui leur est le plus « naturel » possible – ce que n'est pas une salle de classe. Il a d'ailleurs introduit la notion de contexte domestique dans l'étude de la réception, et affirmait ce qui suit à ce sujet :

> *We should not think of every individual as a monad whose opinions crystallize in isolation, or as being in a vaccum (from which processes of group dynamics, for example, are absent). Rather, realistic research would have to come as close as possible, in its methods of research, to*

> *those conditions in which actual opinions are formed, held and modified.*[52]

Nous avons donc envoyé aux répondants sélectionnés un lien qui leur permettait d'effectuer un visionnage de la série, et avons mené auprès d'eux des entrevues individuelles. Nous comprenons cependant que le choix de cette méthodologie offre certaines limites relatives à la collecte des données.

En premier lieu, il est important de souligner que même si nous avons tenté d'offrir un environnement de visionnage « naturel » à nos répondants, l'exercice auquel on leur a demandé de se prêter n'a quant à lui rien de « naturel ». En effet, nous avons demandé à notre auditoire de partager avec nous leurs impressions et leur interprétation de messages médiatiques, alors qu'au terme d'un visionnage « normal », ils ne devraient pas se soumettre à cet exercice. Un effort a donc été demandé, et une situation « exceptionnelle » a ainsi été créée; c'est ce que précise le chercheur Dayan (2000) lorsqu'il évoque « l'artefact spécifique » ou une « prise de parole critique chez des spectateurs pour lesquels une telle performance est exotique ou incongrue ». (Dayan, 2000, p. 438)

Néanmoins cette méthodologie dans le domaine de la recherche a fait ses preuves et permis notamment de confirmer le rôle « actif » du public des médias.

> *L'analyse des publics des médias et de la façon dont ils recevaient leurs messages a tout de suite montré que les individus n'étaient pas des êtres passifs soumis au pouvoir des médias. Ils manifestent au contraire des facultés différentes d'attention, de compréhension, d'interprétation, d'acceptation ou de refus dans lesquelles leur situation personnelle et sociale joue un grand rôle* [53]

---

[52] *Op. cit.*

[53] Ségur, Céline. (2015). *L'étude des publics de télévision en SIC. Quelle évolution conceptuelle ?, Revue française des sciences de l'information et de la communication* [en ligne], 7 | 2015. DOI : 10.4000/rfsic.1470. Récupéré de : *http://rfsic.revues.org/1470*

La deuxième limite qui nous apparaît importante de préciser a trait au choix même d'une approche « qualitative ». Nous pensons certes que ce choix trouve sa légitimité dans le fait que cette méthodologie convient particulièrement à l'objet de notre étude. En effet, cette approche offre « différentes techniques d'interprétation qui peuvent servir à décrire ou à traduire les phénomènes sociaux et qui permettent de porter attention à la signification des phénomènes plutôt qu'à leur fréquence[54] ». Cependant, on peut se questionner sur le caractère subjectif de cette approche : le chercheur ne peut être totalement « neutre » ou complètement « objectif ». À ce sujet, nous pensons que l'argumentaire d'Anadón et Guillemette (2006) répond à ce questionnement lorsqu'ils affirment que « le chercheur ne peut pas faire complètement abstraction de ses "préjugés" et de sa perspective théorique (ou de sa sensibilité théorique)[55] ».

Ajoutons que nous avons gardé en tête que le « chercheur approche le terrain avec des éléments théoriques qui vont lui permettre de sélectionner les situations dans lesquelles il va recueillir les données jugées pertinentes » (Glaser et Strauss, 1967). C'est pour cela que nous avons adopté, en amont de la sélection de notre échantillonnage, des références théoriques compatibles avec notre objet de recherche, et académiquement validées.

Nous sommes finalement consciente que notre échantillonnage demeure restreint et tributaire de nos propres cadres de référence, et que cela limite la portée de nos résultats et donc de notre étude. Il est certain que d'autres chercheurs qui tenteraient de répondre à la même question de recherche pourraient avoir recours à des approches différentes, et ainsi obtenir des résultats autres. Cependant nous croyons que la pluralité des approches ne diminue pas la pertinence de notre propre démarche.

---

[54] *Ibid.*

[55] Anadon, M. et Guillemette, F. (2006). La recherche qualitative est-elle nécessairement inductive? *Recherches qualitatives* 5 (2006): 26-37. Récupéré de http : *//www.recherche-qualitative.qc.ca/Revue.html*

3.5 Composition de l'échantillon

Nous avons constitué notre échantillon en sélectionnant sept personnes qui répondaient aux critères que nous avions définis. Ces personnes ont répondu à l'appel que nous avons lancé dans notre réseau et qui, à notre demande, a également été diffusé dans les différents réseaux de nos contacts.

Les personnes sélectionnées devaient également préalablement accepter de visionner les cinq épisodes de la série au cours de la période que nous avons allouée à cette étape de notre recherche, et accepter de se soumettre aux entrevues individuelles.

Comme nous l'avons vu précédemment, le public cible de la série *Hackers* serait masculin, jeune, éduqué et nanti[56]; cette donnée se précise dans le public cible de la chaîne ICI Explora qui, selon l'information trouvée lors de nos recherches, cible *les hommes âgés de 25 à 54 ans*[57].

Aux fins de notre recherche, nous avons choisi de ne pas restreindre notre échantillon à ce public cible, et élargir notre public afin qu'il couvre différents profils d'usagers d'Internet. Nous justifions ce choix d'une part par le fait que la cybercriminalité est un phénomène qui concerne toute personne utilisant Internet et, d'autre part, par une précision faite par le réalisateur, qui a souligné que la série était destinée et conçue pour un public plus large que celui ciblé par la chaîne : « On s'adresse aux gens qui vont dans le cyberespace », nous a-t-il dit. Cette précision nous a donc conforté dans notre choix d'élargir notre public de façon que notre échantillon soit représentatif des différents usagers du cyberespace.

On peut considérer qu'une partie des profils de nos répondants (la mère, l'aîné, l'adolescente)[58] représente un public secondaire pour la série et que l'autre partie des

---

[56] *Op. cit.*

[57] Lien Multimedia. (2013) *Explora lance une campagne ciblant les amateurs de sports.* Récupéré de *http://www.lienmultimedia.com/spip.php?article36211*

[58] Voir la présentation de l'échantillon dans le chapitre 4.

répondants (le jeune professionnel, le *geek,* l'étudiant, le réfractaire[59]) correspond au public cible, cela confère à notre échantillon une forme de représentativité par rapport au public « réel » de la série.

Nous tenons également à préciser que le profil *anarchiste* a finalement au fil de nos recherches évolué pour correspondre à une réalité plus présente chez les « non-usagers » d'Internet, et plus compatible avec notre objet de recherche, à savoir celui d'une personne réfractaire aux réseaux sociaux et limitant ses interactions dans le cyberespace pour des raisons non économiques mais liées à des « valeurs » (Ram, 1987, 210). Il nous paraît important à cette étape, et afin de justifier notre échantillon, d'expliquer la démarche qui nous a menée à ce choix.

Lors de la construction de notre échantillon, nous nous sommes intéressés aux études menées sur les usagers des technologies de l'information, et plus précisément Internet. Nous avons relevé ce qui suit lors de nos recherches :

> *L'organisme statistique national du Canada a également élaboré une typologie dans le cadre de son enquête sur l'utilisation d'internet en 2005 (Cohendet et al. 2005). Trois groupes de non-usagers ont été identifiés : 1) Le groupe des « non-utilisateurs radicaux ». Il s'agit de personnes généralement assez âgées (plus de 65 ans) et/ou aux revenus très modestes qui ne voient aucun intérêt à investir dans un accès quelconque à internet. 2) Le groupe des « utilisateurs potentiels distants ». Il s'agit de personnes généralement âgées de 55 à 65 ans, qui n'ont pas les compétences pour utiliser internet et peu de motivations pour le faire. 3) Le groupe des « quasi-utilisateurs » qui, pour des raisons de moyens ou de situation géographique (dans des zones rurales ou montagneuses), n'ont pas encore accès à internet, mais sont désireuses de trouver les moyens de se connecter.*[60]

---

[59] Le profil « anarchiste » a évolué en profil « réfractaire ».

[60] Boutet, A. et Tremenbert, J. (2009). Mieux comprendre les situations de non-usages des TIC. Le cas d'internet et de l'informatique. *Réflexions méthodologiques sur les indicateurs de l'exclusion dite numérique », Les Cahiers du numérique,* 2009/1 (Vol. 5), p. 69-100. Récupéré de *https://www.cairn.info/revue-les-cahiers-du-numerique-2009-1-page-69.htm*

Dans cette classification, ce sont essentiellement des déterminants sociaux, économiques ou démographiques qui déterminent la catégorisation des non-internautes. Or, dans le cadre de notre recherche, nous pensions qu'il serait plus pertinent d'inclure le positionnement face à la technologie comme facteur déterminant, et d'avoir accès à un profil de « non-utilisateur par choix ».

En effet, rappelons que la série documentaire *Hackers* traite de la cybercriminalité liée aux réseaux sociaux et à l'émergence des identités numériques. Nous avons donc décidé d'orienter davantage notre recherche vers un profil manifestant une *résistance* à ces réseaux sociaux considérés comme une innovation technique des modes de communication. Notre choix fut d'ailleurs conforté par la lecture de l'étude d'Annabelle Boutet et Jocelyne Trémenbert (2009) qui, en ce qui concerne la classification des « non-usagers », rappelle ce que Sudha Ram a proposé en 1987 comme modèle de résistance à l'innovation. Ram s'est d'ailleurs lui-même inspiré des travaux de Zaltman et Wallendorf (1983) en définissant la *résistance à l'innovation* comme suit : « Toute conduite qui sert à maintenir le statu quo, associé au degré avec lequel les individus se sentent menacés par le changement [...] La résistance à l'innovation n'est autre qu'une version spéciale de la résistance au changement[61] ». Cette réflexion au sujet de la sélection des répondants souhaités dans le cadre de notre recherche nous a donc orienté vers une redéfinition des critères de sélection du *profil 7,* qui a évolué en ce qui suit :

Profil 7) Le/La résistant(e)/réfractaire

Personne qui limite ses interactions sociales. N'ayant pas de comptes Facebook, Instagram, Twitter ou Snapshat, elle revendique la non-utilisation des réseaux sociaux en favorisant les interactions « humaines » plutôt que virtuelles. Personne ne souhaitant pas exposer des informations personnelles sur Internet.

---

[61] *Ibid.*

3.6 Rédaction des questionnaires

Comme indiqué précédemment, nous avons mené plusieurs entrevues individuelles avec les sept répondants sélectionnés pour cette étude. Afin de respecter la méthode de l'entretien semi-directif, nous avons établi un questionnaire général divisé en cinq chapitres, correspondant aux cinq épisodes de la série. Les questions ont évolué en fonction des réponses obtenues lors des entrevues. La figure ci-dessous présente le questionnaire initial tel qu'établi avant la réalisation des entrevues. Nous avons décidé, en raison de la longueur des entrevues, de ne pas les reproduire dans ce mémoire mais d'en donner des extraits pertinents lors de la présentation de l'analyse des réponses des répondants.

Figure 3.1. Questionnaire

Section 1 : Informations sociodémographiques

Âge	
Sexe	
Statut marital	
Profession	
Niveau d'éducation	

Section 2 : Le vol d'identité

Avez-vous visionné l'épisode 1?
Quel est le sujet de cet épisode?
Que savez-vous du vol d'identité ?

Avez-vous déjà été victime d'un vol d'identité ou connaissez-vous quelqu'un qui en a été victime?

Utilisez-vous un réseau sécurisé pour vous connecter?

Vous connectez-vous dans les lieux publics?

Changez-vous régulièrement de mot de passe?

Quels sont selon vous les meilleures pratiques pour éviter de se faire voler son identité?

Qu'avez-vous retenu de cet épisode?

Êtes-vous surpris de ce que vous avez vu et entendu?

Est-ce que vous allez changer vos habitudes de connexion à la suite de ce visionnage?

Qu'allez-vous faire?

Allez-vous en parler à vos proches?

Section 3: Le viol virtuel et la cyberintimidation

Avez-vous visionné l'épisode 2?

Avez-vous aimé cet épisode?

Avez-vous un cellulaire intelligent?

Avez-vous des applications sur votre cellulaire?

Les utilisez-vous fréquemment?

Votre cellulaire est-il protégé par un mot de passe?

Votre cellulaire est-il crypté?

Vous a-t-on déjà piraté votre compte Facebook /Instagram/courriel ou autres?

Comment l'avez-vous découvert ?

Qu'avez-vous fait?

Qu'avez-vous retenu de cet épisode?

Quelles sont pour vous les meilleures pratiques pour éviter de se faire voler ses informations?

Allez-vous changer vos habitudes à la suite de ce visionnage?

Qu'allez-vous faire?

Êtes-vous surpris par ce que vous avez vu et entendu?

Allez-vous en parler autour de vous?

Section 4: Les États

Avez-vous visionné l'épisode 3?
De quoi parle cet épisode?
Connaissiez-vous ces événements ou en avez-vous entendu parler?
Avez-vous été victime d'une cyberattaque connue?
Pensez-vous que les cyberattaques sont réellement dangereuses pour la sécurité du pays?
Pensez-vous que le gouvernement doit mieux se protéger contre les cyberattaques?
Pensez-vous qu'une cyberguerre soit en cours?
Pensez-vous qu'il faille s'inquiéter?
Quel est selon vous la solution pour se protéger contre une cyberattaque?
Quel est selon vous la chose à retenir de cet épisode?

Section 5 : Les entreprises

Avez-vous visionné l'épisode 4?
Que connaissez-vous de la cybersécurité?
Pensez-vous que votre banque est sécurisée?
Pensez-vous que votre entreprise ou celle de vos proches est sécurisée?
Qu'avez-vous appris dans cet épisode?
Êtes-vous surpris par ce que vous avez vu et entendu?
Comment pensez-vous que l'on peut sécuriser une entreprise?
Allez-vous changer vos habitudes à la suite de ce visionnage?
Qu'allez-vous faire?
Allez-vous en parler autour de vous?

Section 6: Les *hacktivistes*

Avez-vous visionné l'épisode 5?
Connaissiez-vous le *hacktivisme* avant de visionner cet épisode?
Comment les *hacktivistes* réussissent-ils à atteindre leurs objectifs?

Comment font-ils pour ne pas se faire prendre?
Pensez-vous que le *hacktivisme* est condamnable?
Est-ce qu'il y a plusieurs types de *hacktivisme*?
Pensez-vous qu'il soit nécessaire ou utile dans certaines situations?
Quelle est la chose qu'il faut retenir de cet épisode selon vous?
Vous sentez-vous à l'abri des *hacktivites*?
Avez-vous peur des *hacktivistes*?
Allez-vous en parler autour de vous?
Allez-vous changer vos habitudes à la suite de ce visionnage?
Qu'allez-vous faire?
Qu'avez-vous retenu de cet épisode?

3.7 Échéanciers des travaux et étapes de recherche

Nous allons détailler, dans ce chapitre, les différentes étapes de notre recherche. La première phase de la recherche a débuté au mois d'avril et s'est déroulée sur une période de trois semaines. Il s'agissait pour nous d'une étape très importante, car elle concernait notre « appropriation » de l'objet de recherche. En effet, nous avons visionné pendant cette période les épisodes de la série documentaire *Hackers*.
La deuxième étape consistait à sélectionner les répondants qui participeraient à notre recherche. Nous avons donc mis en ligne au mois de mai un appel à des participants.
Une demande de certification éthique fut déposée au mois de mai et obtenue au terme de plusieurs ajustements exigés par le jury. En date du 16 mai 2017, nous avons reçu notre certification éthique, ce qui nous a permis de passer à l'étape suivante de recrutement des participants à notre recherche.
L'appel à des participants a été mis en ligne sur les réseaux sociaux et envoyé par courriel à des membres de notre réseau, à qui nous avons demandé de le faire circuler dans leurs réseaux respectifs. Cette première phase de recrutement nous a permis de

sélectionner 5 des 7 répondants de notre étude et les deux autres répondants ont été recrutés au terme d'un second envoi.

Les interactions avec les répondants se sont déroulées par échanges de courriel jusqu'à la rencontre initiale, que nous avons effectuée avec chaque répondant afin de leur permettre de poser les différentes questions qu'ils pouvaient avoir au sujet de la recherche et de leur faire signer les formulaires de consentement.

La figure ci-dessous représente *l'appel à participants* tel qu'il a été envoyé dans les réseaux.

Figure 3.2 - Appel à participants

Candidats recherchés dans le cadre d'un projet de recherche de maîtrise

Je suis candidate à la maîtrise en communication internationale et interculturelle sous la direction du professeur Claude-Yves Charron. Dans le cadre de mon projet de recherche intitulé *Comment la série documentaire* Hackers *communique, sensibilise et éduque sur les grands enjeux liés à la cybersécurité et aux identités numériques?,* je recherche des participants bénévoles et correspondant à différents profils afin de visionner la série *Hackers* et répondre à des questions en lien avec le visionnage, ainsi que des questions sur leurs habitudes de consommation d'Internet. Ce sera une entrevue qui devrait durer trois heures maximum, et qui se déroulera à l'Université du Québec à Montréal.

Si vous répondez à un de ces profils et que vous souhaitez participer, prière de me contacter à mon courriel nacersara@gmail.com

La participation est bénévole et les résultats de la recherche seront diffusés dans le mémoire de maîtrise. Les questionnaires sont anonymes, et aucune information personnelle ne sera diffusée.

Profils recherchés:

Profil 1/ Vous avez entre 19 et 30 ans, et êtes étudiant(e). Vous utilisez fréquemment Internet, notamment pour vos recherches académiques, avez un compte sur les réseaux sociaux et utilisez différents services sur Internet, par exemple des services bancaires. Vous vous connectez souvent à des réseaux publics, notamment dans des cafés, afin de profiter d'une connexion à moindre coût.

Profil 2/ Vous êtes à la retraite, et avez donc du temps libre. Vous avez un compte de courriel et vous vous connectez avec vos petits-enfants ou enfants qui vivent à distance de chez vous. Vous utilisez Internet de manière peu fréquente, mais avez accès à certains services via le Net.

Profil 3/ Vous êtes mère, et utilisez Internet plutôt fréquemment, mais vous êtes une personne très occupée. Vous considérez Internet comme une source d'informations pratique. Vous avez des enfants qui se connectent et vous vous intéressez de près à leur usage d'Internet.

Profil 4/Vous avez entre 28 et 40 ans. Éduqué(e) et professionnellement établi(e), vous utilisez Internet de manière très fréquente. Vous suivez l'actualité et êtes au fait de très nombreuses nouvelles concernant le monde ou la société.

Profil 5/ Vous avez une connaissance avancée d'Internet et utilisez très fréquemment différents outils technologiques. Vous êtes connectée à différentes applications et êtes au fait des plus récentes tendances. Vous avez des notions ou des connaissances approfondies dans le domaine du *hacking*.

Profil 6/ Vous êtes une fille âgée de 13 à 17 ans, vivez dans un univers hyperconnecté, possédez un compte Facebook, Snapshat, Instagram. Vous utilisez Internet de manière très fréquente. Vous prenez souvent des selfies.

Profil 7/ Vous utilisez Internet mais vous n'êtes pas présent(e) sur les réseaux sociaux, car vous pensez qu'il est important de limiter les informations et les données que l'on expose sur Internet. Et vous favorisez les interactions en personne plutôt que virtuelles.

Sara Nacer
Candidate à la maîtrise en communication internationale et interculturelle

À la mi-juin, nous avions sélectionné l'ensemble de nos participants et les formulaires de consentement étaient signés. Nous avons effectué la première entrevue avec le réalisateur au mois de juin, et nous avons effectué les sept entrevues semi-directives avec les répondants au cours des mois de juin et juillet, à raison d'une entrevue par semaine. Les entretiens ont été enregistrés à l'aide d'un enregistreur Tascam dr 40, ce qui nous a permis de télécharger les fichiers audio après chaque entrevue, puis d'en faire une copie et de les stocker sur un disque dur crypté, tel que spécifié dans les exigences de la certification éthique.

Nous sommes ensuite passés à la phase de l'analyse des résultats, qui s'est étalée sur une période de deux mois et demi (août, septembre et octobre). Nous rappelons ici que, dans le cadre de notre travail de recherche, nous avons adopté une approche qualitative et, à cette étape de notre recherche, il s'agissait de définir la meilleure méthode pour analyser les données qualitatives recueillies lors des étapes précédentes. À ce sujet, Trudel et Gilbert (1999) soulignent qu'« il existe différentes méthodes d'analyse de données qualitatives mais il n'en existe aucune qui soit meilleure que les autres. » (Trudel & Gilbert, 1999)

« L'analyse des données qualitative – dont la plus connue est l'analyse de contenu – est la méthode la plus répandue pour étudier les interviews ou les observations qualitatives », écrivait Krippendorff en 2003). Cette information nous a incitée à opter pour l'analyse de contenu. Et, afin de baliser notre démarche, nous nous

sommes basés sur un ouvrage de référence dans le domaine de la recherche, à savoir *L'analyse de contenu,* de Laurence Bardin. Cet ouvrage a été très utile à la bonne marche de notre recherche.

> *L'analyse de contenu est un ensemble d'instruments méthodologiques de plus en plus raffinés et en constante amélioration s'appliquant à des « discours » extrêmement diversifiés et fondé sur la déduction ainsi que l'inférence. Il s'agit d'un effort d'interprétation qui se balance entre deux pôles, d'une part, la rigueur de l'objectivité, et, d'autre part, la fécondité de la subjectivité.*[62]

Nous avons suivi chronologiquement les différentes étapes préconisées. « L'analyse de contenu s'organise autour de trois phases chronologiques : la préanalyse, l'exploitation du matériel ainsi que le traitement des résultats, l'inférence et l'interprétation » (Krippendorff, 2003) Mais avant de pouvoir procéder à la préanalyse de notre corpus, nous avons dû passer par une étape préliminaire essentielle, à savoir la transcription des données.

3.7.1 Transcription des données

Cette étape est primordiale pour tout chercheur ayant mené des entrevues, car elle sert à « faire l'inventaire des informations recueillies et les mettre en forme par écrit[63] ». En effet, au fil de nos entrevues, nous avions récolté des données sous forme d'enregistrements audio, et nous avions également obtenu un enregistrement vidéo de l'entrevue réalisée avec un de nos répondants par le logiciel de vidéoconférence Skype. Il s'agissait donc pour nous de rédiger tout le matériel recueilli par écrit. « Ce texte – appelé verbatim – représente les données brutes de l'enquête. La

---

[62] Bardin, L. (1977) *L'analyse de contenu,* France : PUF

[63] Wanlin, Philippe. (2007). L'analyse de contenu comme méthode d'analyse qualitative d'entretiens: une comparaison entre les traitements manuels et l'utilisation de logiciels. *Recherches qualitatives 3* (2007): 243-272. Récupéré de *http://www.recherche-qualitative.qc.ca/documents/files/revue/hors_serie/hors_serie_v3/Wanlin2.pdf*

retranscription organise le matériel d'enquête sous un format directement accessible à l'analyse[64] ». À cette étape, il était également important pour nous de respecter nos engagements de confidentialité, et ce, en effaçant les données audio et vidéo au terme de la transcription écrite, celle-ci facilitant de plus l'analyse des données. « Il est préférable de les mettre à plat par écrit pour en faciliter la lecture et en avoir une trace fidèle ». (Auerbach, Silverstein, 2003)

La retranscription des données a duré quatre semaines, au terme desquelles nous avons pu passer à l'étape de la préanalyse, tel qu'indiqué dans l'ouvrage de Laurence Bardin. Rappelons que nous avons transcrit huit entrevues, une avec le réalisateur et sept avec les répondants.

3.7.2 Préanalyse

La préanalyse nous a permis de nous familiariser avec notre corpus. Le chercheur Philippe Wanlin la considère d'ailleurs comme « l'étape préliminaire d'intuition et d'organisation pour opérationnaliser et systématiser les idées de départ afin d'aboutir à un schéma ou à un plan d'analyse[65] ».

Nous avons donc effectué une « lecture flottante pour faire connaissance avec les documents » (Robert et Bouillaguet, 1997), ce qui concrètement consistait à « lire et relire pour tenter de bien saisir leur message apparent » (Savoie-Zajc, 2000). Cette préanalyse nous a également permis de bien nous préparer à l'étape suivante car, même si les entrevues ont été réalisées sensiblement à la même période, il était difficile pour nous de faire un lien entre les différentes réponses que nous avions obtenues. La lecture des *verbatim* nous a ainsi permis de cerner de manière globale les éléments des entrevues qui nous serviraient à établir une catégorisation.

---

[64] *Ibid.*

[65] *Op. cit.*

3.7.3 L'exploitation du matériel

L'étape de l'exploitation du matériel a pris la forme d'un exercice assez complexe et a nécessité une grande concentration, car elle exigeait de tenir compte à la fois de notre corpus, de notre objectif de recherche, de nos références théoriques et des différents épisodes de la série documentaire *Hackers.* Cette étape se divise elle-même en deux phases, suivant le mode opératoire suggéré par Laurence Bardin : *l'opération de catégorisation* et *le codage.*

« Le but poursuivi durant cette phase centrale d'une analyse de contenu consiste à appliquer, au corpus de données, des traitements autorisant l'accès à une signification différente répondant à la problématique mais ne dénaturant pas le contenu initial » (Robert & Bouillaguet, 1997). Nous avons établi notre catégorisation sous forme de grille. Cette catégorisation prenait en considération les « caractères communs » (Bardin, 1977) que l'on retrouvait dans notre corpus. « Il s'agit donc de la classification d'éléments constitutifs d'un ensemble par différenciation puis regroupement par genre (analogie), d'après des critères définis afin de fournir, par condensation, une représentation simplifiée des données brutes » (ibid.).

Comme indiqué précédemment, cette étape exigeait une extrême concentration mais également une capacité à synthétiser les données présentes afin de pouvoir établir une catégorisation cohérente et pertinente. Nous tenons à préciser qu'en raison du fait que nous nous intéressions à des thématiques liées à la cybercriminalité, nous avons établi notre « catégorisation » et nos « unités d'enregistrement » en fonction de « thèmes significatifs » abordés dans *Hackers,* mais également en nous basant sur nos questionnaires, afin de faire concorder nos thématiques. Rappelons ici les règles édictées par Berelson (1952) pour la classification catégorielle : « homogénéité, exhaustivité, exclusivité, objectivité et pertinence ».

La seconde phase de l'exploitation du matériel consistait à effectuer le « codage », qui consiste à appliquer « les catégories au corpus ». Cette opération exige d'effectuer une lecture détaillée des différents verbatim, afin de « déterminer le contenu retenu

pour le faire entrer dans la grille d'analyse » (ibid.). En résumé, nous avons, à partir d'une « *grille d'analyse catégorielle* », effectué une lecture détaillée et un « balayage » de notre verbatim. Cela nous a permis de déterminer « les répétitions fréquentielles thématiques ». Nous avons ensuite « découpé le texte en unités », que nous avons ensuite « classées en catégories selon des regroupements analogiques ». Rappelons ici que, tout au long de ces étapes, nous avions comme référence les réponses du réalisateur, la catégorisation du questionnaire et les épisodes de la série *Hackers,* qui servaient de balises afin que la lecture des résultats puisse répondre à notre objectif de recherche.

3.7.4 Traitement, interprétation et inférence des données

À cette étape de notre recherche, nous avons traité les données pour en faire ressortir des éléments significatifs regroupés dans les tableaux de résultats, qui nous ont permis d'entreprendre notre analyse. Ce que nous devions prendre en considération à cette étape, c'était donc l'aspect « significatif » de nos données. Nous cherchions à donner du « sens » à ce que nous avions collecté et catégorisé.

Comme le rappellent Robert et Bouillaguet (1997), l'interprétation des résultats consiste à « prendre appui sur les éléments mis au jour par la catégorisation pour fonder une lecture à la fois originale et objective du corpus étudié » (Robert et Bouillaguet, 1997, p. 31). Les résultats de cette étape sont présentés dans les chapitres suivants.

3.8 Considérations éthiques liées à la méthode

Il était nécessaire d'obtenir une certification éthique de la part du Comité d'éthique de la recherche pour les projets étudiants impliquant des êtres humains (CERPE) de l'UQAM.

Nous considérons cette étape non seulement nécessaire sur le plan académique afin de valider nos entrevues, mais elle nous a également permis de nous préparer à ces entrevues. En effet, pour obtenir ce certificat, il fallait que l'on valide plusieurs étapes du processus de recherche en prenant en considération l'aspect éthique.

Nous avons ainsi dû justifier, entre autres, les critères de sélection de nos répondants, détaillé notre démarche de chercheur et faire approuver chaque étape de notre recherche. Cela concernait également le mode de collecte des données et la confidentialité de ces dernières. Cette étape nous a ainsi permis de valider nos critères de sélection des répondants (genre, âge), et ce, afin d'assurer le principe de « justice et équité dans la participation à la recherche.[66] » Nous avons également rédigé et fait valider nos formulaires de consentement, qui ont été signés par la suite par nos répondants. Nous nous sommes également assuré qu'il n'y avait aucun conflit d'intérêt « réel, potentiel ou apparent[67] ». Cette certification éthique met également l'accent sur l'aspect « vie privée et confidentialité[68] » des répondants; nous nous sommes donc engagés à assurer l'anonymat de nos participants, et à protéger les informations recueillies lors des différentes entrevues. Nous avons ainsi supprimé l'ensemble de nos données audio et vidéo une fois terminée l'étape de la transcription.

Ajoutons que ce processus de certification exigeait de nous que nous nous engagions à exclure de nos entrevues tout jugement et à y maintenir un climat respectueux et ouvert où une position d'« autorité » serait forcément exclue.

---

[66] Instituts de recherche en Santé du Canada. (2014). *Énoncé de politique des trois Conseils : Éthique de la recherche avec des êtres humains, décembre 2014.* Récupéré de *http://www.ger.ethique.gc.ca/pdf/fra/eptc2-2014/EPTC_2_FINALE_Web.pdf*

[67] *Ibid.*

[68] *Ibid.*

CHAPITRE IV

ANALYSE

Nous allons maintenant présenter l'analyse de nos résultats. Nous verrons d'abord, à partir des éléments qui sont ressortis de l'entrevue avec le réalisateur de la série *Hackers*, les messages clés qu'il a voulu véhiculer par la série. Puis nous présenterons notre échantillon de répondants, en précisant les caractéristiques sociodémographiques et économiques propres à chacun. Nous présenterons ensuite les résultats des entrevues réalisées avec nos répondants, en précisant quels types d'usagers d'Internet ils représentent.

Cette analyse des résultats de notre recherche nous permettra de déterminer les « éléments marquants » de la série qui ont retenu l'attention de nos répondants et quels sont, à leurs yeux, les messages clés de chaque épisode de cette série. Cette perception des « récepteurs » de la série (ils en font le « décodage ») sera par la suite confrontée à la perspective du réalisateur lui-même (qui en a fait le « codage »). Car rappelons que nous avons adopté l'analyse communicationnelle développée par Stuart Hall, basée sur la notion de « codage/décodage ».

Rappelons ici que notre question de recherche est *Comment la série Hacker communique, sensibilise et éduque sur les grands enjeux liés aux identités numériques et à la cybercriminalité?*

4.1 Objectifs de la série documentaire *Hackers*

L'entrevue avec le réalisateur, dont la retranscription complète est donnée en annexe de ce mémoire, nous a permis de mettre en lumière l'intention première du réalisateur, et particulièrement ses objectifs communicationnels dans la série *Hackers.*

> *En tant que série, au départ, c'était de vulgariser cette espèce de personnage que les médias décrivent des fois comme un criminel, des fois comme un révolutionnaire, des fois comme un espion, qui est le* hacker. *Ça fait quoi un* hacker *dans la vie ? C'est quoi, les différentes façons d'être un* hacker *? Et c'est quoi les différents moments de la vie où, comme citoyens, on peut être confrontés à ces phénomènes-là. Donc ça, c'est le truc de départ : qu'est-ce que ça mange en hiver, un* hacker *? comme dirait l'expression québécoise. Après ça, il fallait décliner ça en cinq champs d'activité*[69].

La série est donc, selon lui, consacrée à faire connaître le phénomène du *hacking* en le vulgarisant auprès du public, et en mettant en lumière les différents champs d'activité touchés par ce phénomène. L'intention première de la série est donc d'*informer* l'auditoire de l'existence de ce phénomène mais également de le *sensibiliser* aux différents dangers auxquelles il s'expose dans le cyberespace.

Nous avons tenté, avec le réalisateur, de préciser ces thèmes dans chaque épisode.

---

[69] Nacer, S. (2017, 6 juin). Entrevue avec Bachir Bensaddek sur la série documentaire *Hackers*, Montréal, QC.

4.1.1 Épisode 1 : Le vol d'identité

Le premier épisode s'intéresse au vol d'identité susceptible de toucher toute personne qui se connecte sur Internet.

> *La plupart des gens ne sont pas protégés pour faire face à des pirates informatiques. Accompagné d'un hacker, Matthieu Dugal va se promener à bord d'une camionnette banalisée à la recherche de victimes, afin de voler des informations personnelles. Dans un café, dans un dépanneur, ils vont mettre la main sur des numéros d'assurance sociale, des comptes de banque, des photos de vacances, des mots de passe.*[70]

C'est donc à travers des exemples concrets de vol d'informations personnelles auprès de personnes qui se connectent dans des réseaux publics non sécurisés, ou par le piratage de réseaux domestiques non sécurisés, de même qu'en utilisant certains objets connectés, que l'animateur expose les différentes façons d'accéder aux données personnelles, et cela, en présence d'experts qui vulgarisent et expliquent les méthodes utilisées par les *hackers.*

Cet épisode *informe* donc l'auditoire sur l'existence de failles dans les systèmes de connexion utilisés quotidiennement, que ce soit dans des espaces privés comme les domiciles ou des espaces publics comme les cafés.

Rappelons à ce sujet que le chercheur Dominic Wolton (2005) soulignait l'importance, selon lui, de distinguer *communiquer* et *informer.*

---

[70] ICI Explora. (2016) *HACKERS.* Récupéré de http://ici.exploratv.ca/emissions/hackers

> *Informer n'est plus synonyme de communiquer. Le plus important, et le plus compliqué, dans la communication, c'est le récepteur. Que ce soit un individu, un groupe, une société. Communiquer aujourd'hui, ce n'est pas seulement transmettre une information, c'est aussi tenir compte du récepteur.*[71]

Il nous apparaît important de mettre en exergue cette distinction, car cela nous a permis de nous questionner davantage sur ce qui caractérise un média communicationnel comme la série *Hackers,* que le réalisateur utilise pour *communiquer* et *informer* son auditoire. Nous reviendrons sur cela lorsque nous aborderons la méthodologie du réalisateur.

Cet épisode traite donc de deux concepts : le *hacking* et *l'internet des objets.* Cet épisode présente en effet le phénomène du *hacking* au public en se concentrant sur ses champs d'activités, qui touchent les individus et qui sont reliés aux modes de connexion que ces derniers utilisent, mais également aux différentes technologies utilisées quotidiennement. Et ces technologies sont intrinsèquement liées à l'émergence de l'*internet des objets.*

Nous avons d'ailleurs questionné le réalisateur afin de relever les éléments à retenir de cet épisode, et voici sa réponse :

> *Ce qu'on voulait sortir de ça, c'est qu'on vit dans un univers connecté, avec de plus en plus d'objets qui sont connectés, et un moment donné il faut se poser la question : qu'est ce qui est enregistré par cette machine ? qu'est ce qui est transmis ? qu'est-ce que je fais avec ça ? Il y a des télés Samsung, dont on s'est rendu compte il n'y a pas longtemps*

---

[71] Wolton, Dominique. (2005). Il faut sauver la communication. *Revista FAMECOS Porto Alegre* nº 27 agosto 2005 quadrimestral. Récupéré de http://revistaseletronicas.pucrs.br/ojs/index.php/revistafamecos/article/viewFile/3317/2574

> *qu'elles enregistraient le son et qu'elles l'envoyaient à la centrale Samsung. C'est sorti il y a quelques mois. On fait quoi avec ça ?*[72]

En approfondissant nos recherches, nous avons effectivement trouvé plusieurs articles confirmant ce que le réalisateur avançait au sujet des téléviseurs intelligents, par exemple dans le très sérieux journal anglais *The Telegraph* qui, dans un article intitulé « Why your smart TV is the perfect way to spy on you », publié en mars 2017, mettait en lumière l'existence de *hacking* à l'aide de téléviseurs intelligents.

> *In a world of internet connected devices that could be targeted by hackers in a number of ways it has become common parlance to hear of smartphones and computers being hacked and turned into spying tools. But recently another common device has been added to the roster of possible monitors: smart TVs.* [73]

Ce que nous révèle également l'entrevue menée avec le réalisateur, c'est que, sur le plan des *messages*, son intention dès le premier épisode était de faire comprendre au public que le *hacking* est un phénomène qui fait partie de notre réalité quotidienne mais qu'on ignore parfois son existence. « On va essayer de montrer qu'on s'en rend pas compte mais, de nos jours, on est surveillés au quotidien sans s'en rendre compte ». Cela nous renvoie d'ailleurs à la réflexion du chercheur Adam Segal (2016) qui, dans ses recherches, a souligné l'importance que prend ce phénomène, en déclarant : « Everybody is spying on everybody else [74] ». Mentionnons cependant que Segal s'intéresse plus

---

[72] Nacer, S. (2017, 6 juin). Entrevue avec Bachir Bensaddek sur la série documentaire *Hacker*, Montréal, QC.

[73] McGoogan, Cara. (2017, 8 mars). Why your smart TV is the perfect way to spy on you. *The Telegraph*. Récupéré de http://www.telegraph.co.uk/technology/2017/03/08/smart-tv-perfect-way-spy/

[74] Segal, Adam. (2016). *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*, New York : Public Affair Tm. Récupéré de http://books.google.com/

particulièrement au *hacking* à l'échelle des nations, alors que la série *Hackers* s'intéresse principalement, dans son premier chapitre, au *hacking* ciblant les individus.

4.1.2 Épisode 2: Le viol virtuel et la cyberintimidation

Le deuxième chapitre de la série, aborde également le *hacking* ciblant les individus, mais il se focalise plus particulièrement sur les personnalités publiques.

> *Autrefois, les paparazzis risquaient leur vie pour prendre des photos floues et mal cadrées de vedettes. Aujourd'hui, il suffit de pirater leur iPhone, leurs courriels et les services de stockage de données en ligne pour avoir accès à leur vie privée.*[75]

Ce qui est ressorti en premier lorsque nous avons abordé cet épisode avec le réalisateur, c'est le caractère divertissant de ce dernier. « C'était l'épisode que je te dirais le plus divertissement, parce qu'on prend une personnalité célèbre et puis on lui lance un défi »[76]

Néanmoins il a tenu à souligner que le *hacking* qui cible certaines vedettes n'était pas un phénomène isolé, puisqu'à travers l'émergence des réseaux sociaux, il y avait également l'émergence de personnalités publiques. « Il y a des personnages qui sont pas du tout des célébrités, des personnages publics, mais qui deviennent des célébrités sur les réseaux sociaux ».[77]

---

[75] ICI Explora. (2016) *HACKERS.* Récupéré de http://ici.exploratv.ca/emissions/hackers
[76] Nacer, S. (2017, 6 juin). Entrevue avec Bachir Bensaddek sur la série documentaire *Hackers.* Montréal, QC.
[77] Ibid.

Sur le plan théorique, nous mettons ici le doigt sur un phénomène que les chercheurs en sociologie surnomment la « reconnaissance de singularités subjectives »[78]. En effet, l'étude comportementale des usagers nous apprend qu'à travers les réseaux sociaux, « les sujets ne peuvent parvenir à une relation pratique avec eux-mêmes que s'ils apprennent à se comprendre à partir de la perspective normative de leurs partenaires d'interaction, qui leur adressent un certain nombre d'exigences sociales » (Honneth, 2008, p. 113). Cela explique l'importance que les gens accordent à l'image projetée par leurs identités numériques, et cela nous renvoie d'ailleurs aux travaux de Harvey, car ces phénomènes comportementaux émergent « des échanges à l'intérieur des communautés existantes au sein des réseaux sociaux ». (Pierre-Léonard Harvey, 1995).

Certaines identités virtuelles confèrent à leur propriétaire une grande notoriété, qui va davantage les exposer aux risques de *hacking* en en faisant des cibles potentielles pour les *hackers*. Cet épisode s'intéresse donc particulièrement au *hacking* touchant les personnalités publiques, en nous démontrant les risques auxquelles elles sont exposées par leur statut mais, pour le réalisateur, cet épisode s'adresse également à toute personne faisant usage des réseaux sociaux. Cet épisode traite donc, comme le premier, de *hacking* ciblant les individus.

> *Il est très en lien avec le premier épisode, mais je te dirais que la raison n'est pas la même. Là, c'est la prise de contrôle de la vie de quelqu'un qui est plus exposé et à qui on explique comment il devrait se protéger, mais ça vaut aussi pour le commun des mortels, c'est à dire t'as beau ne pas être un personnage public, faire attention à tes mots de passe,*

[78] Granjon, F. et Denouël, J. (2010) Exposition de soi et reconnaissance de singularités subjectives sur les sites de réseaux sociaux. *Sociologie,* 2010/1 (Vol. 1), p. 25-43. DOI : 10.3917/socio.001.0025. Récupéré de https://www.cairn.info/revue-sociologie-2010-1-page-25.htm

> *sécuriser le wifi à la maison, t'assurer que tes machines ne sont pas complètement vulnérables, c'est un minimum.*[79]

4.1.3 Épisode 3: Les États

Le troisième épisode de la série Hacker explore la cybercriminalité à l'échelle des États. Ce chapitre marque donc le passage du *hacking* ciblant les individus au *hacking* ciblant les nations.

> *Aujourd'hui, certaines guerres font beaucoup de dégâts invisibles. Un virus informatique a déjà attaqué une centrale nucléaire en Iran alors qu'un autre a bloqué l'électricité de toute une ville en Ukraine. Matthieu Dugal rencontre des experts en cybersécurité et en stratégies politiques afin de mieux comprendre les enjeux de la cyberguerre à une époque où de plus en plus d'objets connectés peuvent devenir des menaces aux mains de puissances mal intentionnées.*[80]

Sur le plan théorique, cet épisode introduit le concept de « cyberguerre », qui est présenté à l'auditoire comme un problème de sécurité nationale majeur. Nous nous sommes intéressée à ses différentes définitions dans la littérature scientifique et avons retenu la suivante, pour sa concordance avec notre sujet de recherche.

> *La cyberguerre peut désigner une opération menée par un État à l'encontre d'une entité non étatique en dehors de son territoire, notamment dans le cadre de la lutte contre le terrorisme, ou encore une offensive terroriste menée à l'initiative d'un groupe non étatique mais destinée à porter atteinte aux intérêts d'un État ou de sa population.*[81]

---

[79] *Op. cit.*

[80] ICI Explora (2016). *HACKERS.* Tiré de http://ici.exploratv.ca/emissions/hackers

[81] Adhami, A. (2007) The Strategic Importance of the Internet for Armed Insurgent Groups in Modern Warfar., *RICR,* vol. 89, n° 868, 2007, p. 864. Récupéré de https://revdh.revues.org/984?lang=en

Notre entrevue avec le réalisateur a permis connaître quels éléments impliquant la « cyberguerre » il avait tenté de mettre en lumière dans cet épisode. Sa réponse a été la suivante :

> *L'idée là-dedans, c'était qu'on se rende compte que finalement nos États sont en conflit pas ouverts, car ils ne veulent pas que ce soit ouvert, parce qu'ils font des choses qui ne sont pas forcément légales. On dit toujours que les Chinois espionnent, mais tout le monde espionne et tout le monde est espionné.*[82]

Cet épisode traite des mêmes enjeux abordés par le chercheur Adam Segal (2016). Cependant le langage propre à ce média télévisé se caractérise par un certain degré de simplification. L'auditoire de la série est sensibilisé à travers cet épisode à l'existence d'une « cyberguerre » touchant les nations et ayant des répercussions diplomatiques. L'épisode évoque notamment l'existence de conflits impliquant la Chine, les États-Unis, la Russie, l'Iran et Israël. Il rappelle par ailleurs certains événements majeurs relatifs à ces conflits, tels que l'implantation du virus *Stuxnet* en Iran. Segal, quant à lui, approfondit davantage dans son œuvre l'analyse de ces conflits à travers l'émergence de la « cyberdiplomatie ». À ce sujet, il met en lumière le concept de « Year Zero », en référence à l'année 2012 qui, selon lui, marque une transformation de la géopolitique et des tactiques des grandes puissances en quête de pouvoir.

> *It was in 2012 that nation-states around the world visibly reasserted their control over the flow of data and information in search of power, wealth, and influence... The conflict in cyberspace will only become more belligerent, the stakes more consequential... We will all be caught in the*

[82]Nacer, S. (2017, 6 juin). Entrevue avec Bachir Bensaddek sur la série documentaire *Hackers*, Montréal, QC.

> *fallout as the great powers, and many of the lesser ones, attack, surveil, influence, steal from, and trade with each other*[83]

Segal explore donc ce changement de paradigmes dans les relations de pouvoir qui résulte de l'émergence de la « cyberguerre » comme nouvelle réalité. Le troisième épisode de *Hackers* explore le *hacking* comme phénomène résultant de cette « cyberguerre ». L'épisode met en évidence l'existence de conflits ayant des répercussions majeures sur la sécurité nationale des États, en soulignant le fait que ces derniers demeurent peu connus du grand public.

Au cours de notre entrevue, le réalisateur a tenu à rappeler les conséquences directes sur les individus du *hacking* touchant les États. Il a également tenu à souligner que des informations sensibles telles que les dossiers de santé des hommes d'État pouvaient être la cible de *hackers* tentant de nuire à la sécurité nationale.

> *Il y a tout ce qui est nos données dans notre État, les impôts les systèmes de santé, les systèmes éducatifs, tout ça c'est des millions et des millions de pages qui sont stockées un peu partout dans des serveurs qui sont pas forcément bien sécurisés, et la sécurité des États elle passe aussi par ça, elle passe par nos données, tu sais le bulletin de santé de notre premier ministre, de notre ministre de la Défense.* [84]

Il a également tenu à rappeler que la sécurité intérieure des États était intrinsèquement liée à sa capacité de protéger les données qui touchent les citoyens. « C'est-à-dire qu'il n'y a pas que la guerre mais il y a la sécurité intérieure. La sécurité intérieure, ça

---

[83] Segal, Adam. (2016). *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age,* New York : Public Affair Tm. Récupéré de http://books.google.com/

[84] ICI Explora (2016). *HACKERS.* Récupéré de http://ici.exploratv.ca/emissions/hackers

joue beaucoup, et ça dépend beaucoup de la façon qu'on a de protéger les données dans nos agences gouvernementales. »[85]

La protection des données est d'ailleurs au cœur des recherches d'Adam Segal qui, dans un article intitulé « New Cyber Brief: Protecting Data Privacy With User-Friendly Software », rappelle que l'augmentation des attaques massives ciblant les données peut avoir de graves conséquences, autant pour les entreprises et les organisations qu'en ce qui concerne la sécurité publique.

> *Protecting the privacy of user data from unauthorized access is essential for business executives, policymakers, and users themselves. The pace of targeted attacks and massive data breaches is only increasing. Each new incident hurts organizations' bottom lines, undermines users' trust in the products they use every day, and can have dire consequences for public safety*[86]

4.1.4 Épisode 4 : Les entreprises

Le quatrième épisode s'inscrit dans la continuité du troisième, puisqu'il explore les questions de *hacking* relatifs à la protection des données, mais à l'échelle des entreprises.

> *Toutes les entreprises sont à la merci des pirates informatiques. La question n'est pas de savoir si elles vont se faire pirater, mais quand, comment et pendant combien de temps ça va se passer. En compagnie d'un expert en cybersécurité, Matthieu Dugal va mener des tests d'intrusion dans les systèmes d'une entreprise bien connue, Téo Taxi. Comment vont-ils procéder pour infecter les machines de l'organisation?*

---

[85] *Ibid.*

[86] Segal, A. (2016, 22 février). New Cyber Brief: Protecting Data Privacy with User-Friendly Software. [Billet de blogue]. Récupéré de https://www.cfr.org/blog/new-cyber-brief-protecting-data-privacy-user-friendly-software

Réussiront-ils à piller des données sensibles? Et comment réagira l'entreprise?[87]

La protection des données personnelles est le sujet principal de ce quatrième épisode. Et, afin de vulgariser pour l'auditoire l'importance de protéger les données sensibles des usagers mais également celles des employés des entreprises, le réalisateur a effectué un test d'intrusion au sein de la compagnie montréalaise Téo. Cette dernière se spécialise dans le transport privé. « C'est une vraie prise de contrôle, un vrai test d'intrusion qu'on avait avec eux et qui a fonctionné[88] ». Nous nous sommes donc intéressée à ce qu'était une intrusion. Dans un document préparé pour le compte du département américain de l'Énergie intitulé *Secure Data Transfer Guidance for Industrial Control and SCADA Systems*, les intrusions sont définies comme suit : « Attacks from outside the organization » and misuse « attacks or malfeasance from within organizations[89] ». Ce document rédigé par des experts en cybersécurité inclut divers recommandations, dont la nécessité pour les compagnies de se protéger contre les attaques en effectuant différents tests d'intrusion, et en mettant en place des systèmes de détection tels que les *Intrusion Detection Systems (IDS)* et les *Intrusion Prevention Systems (IPS).* Gabrielle Desarnaud (2017), chercheuse à l'Ifri[90], et dont les recherches couvrent les enjeux de cybersécurité pour les infrastructures énergétiques, rappelle que l'intrusion demeure un risque omniprésent au sein de toute entreprise intégrant des fonctions numériques. Elle ajoute à ce sujet que les tests d'intrusion ne suffisent pas.

---

[87] ICI Explora. (2016) *HACKERS.* Récupéré de http://ici.exploratv.ca/emissions/hackers

[88] *Ibid.*

[89] Mahan, Robert E., et al. (2011). Secure data transfer guidance for industrial control and SCADA systems. *No. PNNL-20776. Pacific Northwest National Laboratory (PNNL), Richland, WA (US), 2011.* Récupéré de http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-20776.pdf

[90] L'Ifri est, en France, le principal centre indépendant de recherche, d'information et de débat sur les grandes questions internationales.

> *Si la résistance à toutes sortes d'intrusions a été testée au préalable, les experts s'accordent à dire que, de la même manière que pour tout autre objet connecté intégrant des fonctions numériques, l'existence de failles ne peut être exclue... La résilience de nos systèmes énergétiques est donc un aspect essentiel de la cybersécurité*[91]

Lorsque l'on fait le lien avec le quatrième épisode de la série *Hackers,* on comprend que la vulnérabilité des systèmes de gestion au sein des entreprises demeure un problème majeur de cybersécurité. Et c'est ce que le réalisateur a tenté de démontrer en effectuant un test d'intrusion dans une entreprise. Il a ainsi mis en lumière le caractère vulnérable des systèmes informatiques et souligné l'existence de brèches qui permettent d'accéder à des données sensibles telles que les numéros de cartes de crédit des clients. Il a néanmoins tenu à rappeler un fait important pendant l'entrevue, à savoir que l'entreprise Téo avait fait preuve de collaboration et d'ouverture. Il nous a ainsi indiqué que Téo avait accepté d'exposer ses failles et de collaborer avec les experts en toute transparence. « Avec Téo, bien, on les appelés. À partir du moment où on leur a dit : on a les mots de passe et les noms de certaines de vos dirigeants, ça veut dire qu'on est rentrés chez vous, ils nous ont dit : ok, bon d'accord, venez nous voir[92] ».

Cet épisode a également mis en lumière les méthodes utilisées par les *hackers* pour s'introduire dans les systèmes des entreprises. D'ailleurs, selon le réalisateur, ce qu'il fallait retenir de l'intrusion qu'il avait réalisée, c'était qu'« une entreprise qui est « technosoucieuse » de ce qui se passe autour d'elles, peut se faire avoir si tu trouves le bon angle, et le bon angle : c'est l'ingénierie sociale, (social engineering), faut que tu sois un peu vicieux et que tu fasses croire des choses aux gens[93] ». L'épisode a

---

[91] Desarnaud, Gabrielle. (2017) *Faire face au risque,* France : Ifri. Tiré de https://www.ifri.org/sites/default/files/atoms/files/desarnaud_cybersecurite_2017_sl.pdf

[92] Nacer, S. (2017, 6 juin). Entrevue avec Bachir Bensaddek sur la série documentaire *Hackers,* Montréal, QC.

[93] *Ibid.*

ainsi révélé comment l'expert en cybersécurité avait pu s'introduire dans les systèmes de l'entreprise Téo. Il s'agit d'un procédé appelé « hameçonnage » (*phishing*), qui a consisté dans ce cas à faire croire à un employé qu'un courriel avait été envoyé par son patron, et qui lui indiquait de cliquer sur un lien.

> *Le mec, il a créé une adresse Internet qui ressemble beaucoup à celle d'Alexandre Taillefer. Bon, on dit juste « un dirigeant » mais, dans ce cas-là, c'était Alexandre Taillefer, et qui dit : « Mais qu'est-ce que c'est cette pub de Uber ? Ils me matent la laine sur le dos, faut qu'on fasse quelque chose, les gens ils voient le boss ! » Il m'a envoyé un truc et il n'est pas content, et évidemment, t'as ouvert le truc, t'as été voir la pub, et hop voilà, tu es hameçonnée, tu m'appartiens, et je fais ce que je veux avec toi, et ça se déplace partout.*[94]

Le chercheur Christopher Hadnagy, auteur de *Social Engineering: The Art of Human Hacking* (2011), définit le hameçonnage comme étant une pratique basée sur le leurre et permettant d'obtenir des informations personnelles. « A phishing is the practice of sending e-mails that appear to be from reputable sources with the goal of influencing or gaining personal information ». (Hadnagy, 2015) Cela correspond parfaitement au stratagème adopté par l'expert dans cet épisode. Selon le même chercheur, les courriels qui sont utilisés pour créer des intrusions dans les systèmes représentent jusqu'à 90 % des courriels envoyés chaque jour. « Phishing emails are estimated to comprise up to 90 percent of the 300 billion emails sent each day ». (ibid.)

Ce quatrième épisode met en lumière le *hacking* à l'échelle des entreprises, en exposant les vulnérabilités des systèmes d'une part et en révélant les moyens utilisés par les *hackers* d'autre part. Cet épisode souligne également le fait que le *hacking* qui touche les entreprises a une incidence sur les individus, car cela met en péril la protection des données personnelles des usagers faisant affaire avec ces dernières, comme le rappelle le réalisateur.

---

[94] *Ibid.*

> *Ce qu'on voulait montrer, c'est que nos données, en tant qu'individus, en tant qu'usagers, que personnes privées, se retrouvent sur des serveurs qui appartiennent à des compagnies avec qui on fait affaire, comme des banques, comme des compagnies de services et que, si elles sont pas sécurisées, eh bien ça peut nous mettre en danger éventuellement, nous. Eux se mettent en danger, mettent en danger la vie privée de leur employés parce que, finalement, si t'as les mots de passe et les noms d'un usager, tu peux savoir où il vit, tu peux savoir s'il a une double vie, s'il a des enfants, si ses enfants ont des problèmes ou des maladies, s'ils était vraiment en voyage au Mexique ou s'il était à Paris avec quelqu'un d'autre. Tu sais, tu vois tout ça là, tout ça finalement c'est en danger, et toi, usager, ils ont ta carte de crédit*[95].

4.1.5 Épisode 5 : Les *hacktivistes*

Le dernier chapitre de la série s'intéresse aux *hackers* eux-mêmes. Après avoir exploré les conséquences du *hacking* à différentes échelles, le réalisateur a donc décidé de consacrer son dernier épisode aux acteurs responsables du *hacking* plutôt qu'aux victimes. « Ce qu'on voulait, c'était faire un portrait de cette communauté[96] ».

> *Les* hackers *n'ont pas tous des intentions malveillantes. Certains mettent leurs connaissances au service de causes. Si leurs intentions sont justes, leurs procédés ne sont pas forcément légaux. Matthieu Dugal va à la rencontre de ces Robins des bois des temps modernes. En compagnie d'un membre d'Anonymous, il va naviguer dans le « darknet ». Comment les* hacktivistes *réussissent-ils à atteindre leurs objectifs? Comment font-ils pour ne pas se faire pincer? Et quels dangers les* hacktivistes *courent-ils?*[97]

Notre analyse de l'entrevue avec le réalisateur a permis de mettre en lumière les objectifs communicationnels de cet épisode, qui se divisent en deux parties.

---

[95] *Ibid.*
[96] *Ibid.*
[97] ICI Explora (2016). *HACKERS.* Récupéré de http://ici.exploratv.ca/emissions/hackers

Le premier objectif est de mettre en évidence l'existence de deux profils de *hackers* qui se rejoignent dans les moyens utilisés mais qui s'opposent dans leurs intentions. « Je te dirais qu'il y a deux types de *hackers* : il y a Robin des bois, un « hacktiviste », et il y a Scarface, qui fait ça pour sa gueule, pour gagner du fric, voilà. On voulait montrer que ces gens-là, ils utilisaient les mêmes outils finalement[98] »

Sur le plan théorique, nous nous sommes intéressées à un nouveau concept qui a émergé dans cet épisode, à savoir le « hacktivisme ». Selon le sociologue Tim Jordan (2009), les *hacktivistes* sont des militants politiques associés principalement à des mouvements altermondialistes : « Hacktivists are political activists, most often associated with the alter–globalization movement[99] ». Dans un ouvrage publié en 2004, le sociologue Tim Jordan et le maître de conférences en théorie des communications Paul A. Taylor définissaient l'*hacktivisme* comme suit : « Hacktivism is the emergence of popular political action, of the selfactivity of groups of people, in cyberspace. It is a combination of grassroots political protest with computer hacking[100] ». Ils font également le lien entre *hacking* et *hacktivisme* en soulignant que ce dernier est finalement une forme de protestation contemporaine dans un monde hyperconnecté : « Hacktivists are the marriage of the spirit of the hack and the spirit of protest in the context of viral times[101] ».

---

[98] *Op. cit.*

[99] Dasgupta, D. et Ferebee, D. M. (2013). Consequences of diminishing trust in cyberspace. The *Proceedings of the 8th International Conference on Information Warfare and Security:* ICIW 2013. Academic Conferences Limited, 2013. Récupéré de https://books.google.ca

[100] Jordan T. et Taylor, P. (2004) *Hacktivism and Cyberwars: Rebels With a Cause?* London: Routledge. Récupéré de https://books.google.ca

[101] *Ibid.*

Le second objectif de cet épisode est, pour le réalisateur de la série, de démontrer la complexité de ce phénomène. En effet, il met en lumière la difficulté de distinguer *hacker* et *hacktiviste*.

> *Pour les forces de l'ordre et les gens qui les étudient, ils ont les mêmes outils, ils traînent dans le mêmes chat rooms, ils ont les mêmes espaces de dialogue ils sont tous sur 4 chan, ils sont tous sur Reddit, et puis sur les IRC, à discuter.* [102]

Il ajoute que, même en observant leur communications et échanges dans ces différentes plateformes, il demeure difficile de déterminer clairement leurs objectifs et motivations.

> *Mais tu ne sais pas quel est leur objectif, c'est à dire il y en a un, son objectif, c'est d'aller chercher de l'information au sujet du code, pour pouvoir s'attaquer à des corporations, parce qu'il est anti-corporations; et l'autre, bien lui, il veut du code tout simplement parce qu'il veut s'attaquer à des corporations parce qu'il veut aller chercher du fric dans les corporations.* [103]

4.1.6 Communiquer, éduquer et sensibiliser à travers la série documentaire *Hackers*

Cette entrevue nous a permis de mieux saisir la démarche du réalisateur et de connaître ses objectifs communicationnels. Elle nous a également permis de mieux baliser notre entrevue avec nos participants afin que l'analyse de leurs réponses permette de répondre concrètement à notre question de recherche.

---

[102] Nacer, S. (2017, 6 juin). Entrevue avec Bachir Bensaddek sur la série documentaire *Hackers*. Montréal, QC.
[103] *Ibid.*

Le dictionnaire donne du mot « communiquer » la définition suivante : « Faire part de, donner connaissance de quelque chose à quelqu'un, par relation plus ou moins directe avec le destinataire[104] ».

Dans le cas de la série documentaire *Hackers,* notre questionnement en tant que chercheurs en communication concernait l'axe communicationnel privilégié par le réalisateur. Il paraissait donc nécessaire pour nous à cette étape de comprendre l'essence même du documentaire télévisé. Nous nous sommes donc intéressés aux travaux de Sophie Barreau-Brouste, sociologue, spécialiste de la culture et des médias. Dans un dossier[105] publié en France en 2013 pour le compte de l'Institut national de l'audiovisuel, la sociologue revient sur l'évolution du documentaire dans le secteur de l'audiovisuel. Une lecture de sa recherche nous a permis de déterminer les caractéristiques communicationnelles propres à ce média. Elle utilise également des références pertinentes aux travaux de ses pairs.

> *Les œuvres diffusées à la télévision de caractère dit « documentaire » sont composées de séquences visuelles qui transmettent le patrimoine littéraire, scientifique, artistique appréhendé par notre société. Dans le domaine qui nous intéresse, le travail de l'auteur consistera à traduire un fait en images et en sons, et si l'enchaînement des images constitue une relation de cet événement où apparaît un effort de l'auteur pour en exposer une forme personnelle reflétant sa pensée dans l'interprétation qu'il offre des choses, il y aura œuvre de création, donc œuvre de l'esprit investie des droits de l'auteur*[106].

---

[104] Centre national de ressources textuelles et lexicales. (2012) Communication. *Outils et références pour un traitement optimisé de la langue.* Récupéré de http://www.cnrtl.fr/definition/communiquer

[105] Barreau-brouste, S. (2013). *Le documentaire télévisé : les enjeux d'une définition controversée,* Institut national de l'audiovisuel. récupéré de https://www.ina-expert.com/e-dossier-le-documentaire-un-genre-multiforme/le-documentaire-televise-les-enjeux-d-une-definition-controversee.html#5

[106] Mehl, D. (1992) *La fenêtre et le miroir. La télévision et ses programmes,* Paris : Payot, collection « Documents », p. 156. Récupéré de https://www.ina-expert.com

Cette définition du documentaire télévisé de Dominique Mehl (1992) nous éclaire sur le rapport particulier qui lie le créateur du documentaire au sujet exposé. Ainsi, sur le plan communicationnel, nous comprenons que ce qui caractérise la série documentaire, c'est avant tout la personnalisation du message selon la perspective de l'auteur. Dans le cas de notre série documentaire, cela veut dire que le traitement du phénomène de *hacking* est teinté par l'interprétation subjective du réalisateur. C'est-à-dire que les informations transmises dans le documentaire résultent de l'appropriation du sujet par son auteur, et de sa propre compréhension du phénomène. Cela nous renvoie encore une fois aux travaux de Hall, qui soulignait que le *codage* des messages médiatiques se construit autour du cadre de référence du producteur, mais également que le *décodage* dépend du cadre de référence du récepteur. Ce que Barreau-Brouste met également en lumière dans sa publication, c'est l'importance de la narration, qui devient l'élément essentiel dans toute histoire. « Pour les programmateurs, un documentaire est avant tout une histoire qui suscite de l'émotion[107] ». Elle appuie d'ailleurs ses propos en citant le producteur Georges Benayoun (1990) : « Un bon sujet de documentaire, aujourd'hui, raconte une histoire, une aventure humaine. Il faut un auteur qui travaille à la base, sur la narration. Le documentaire a besoin d'émotion[108] ». Nous avons donc voulu comprendre comment le réalisateur de la série *Hackers* avait construit sa narration afin que cela suscite une « émotion » chez son auditoire. Voici sa réponse :

> *Il fallait décliner ça en cinq champs d'activités, et lui donner un style, lui donner un* look. *Et ce qu'on s'est dit, bon, regarde, là c'est la dimension informative : c'est quoi, un* hacker *? On s'est dit : ben, si on fait de la télé, si on fait du docu, faut qu'on donne une petite touche de plus...on va faire peur, on va essayer de faire peur, on va essayer de montrer qu'on s'en rend pas compte mais, de nos jours, on est surveillés au quotidien*

---

[107] *Op. cit.*

[108] Benayoun, G. (1990) « Les hauts et les bas du documentaire français », *Le film français,* n° 2294, 9 février 1990, p. 16. Tiré de https://www.ina-expert.com

> *sans s'en rendre compte, on le sait pas, on abuse de toutes sortes de techniques.*[109]

Il nous révèle qu'il a construit son message en créant une « intrigue » basée sur la « peur ». Ainsi, tout en gardant comme objectif le caractère informatif du documentaire, il a tenté de capter son auditoire à travers un scénario construit autour de différentes intrigues.

Notre entrevue nous a permis également de mieux saisir la logique narrative du réalisateur car, lorsque nous lui avons demandé si finalement sa démarche s'inscrivait dans le champ du loisir, sa réponse a été la suivante :

> *Le loisir, c'est le prétexte, c'est-à-dire on passe par le loisir, que les gens s'amusent en regardant la série, qu'ils aient du plaisir, mais pour leur faire passer l'information qui est la suivante, à savoir que trouver une clé USB par terre et la ramener chez soi, la brancher dans son ordi, aller payer son compte alors qu'on est branché sur le wifi d'un café, aller payer ses factures alors qu'on est branché sur le wifi d'un café, ou encore ne pas sécuriser son réseau à la maison, et puis, tu sais, je sais pas moi, déshabiller ses enfants, donner le bain devant la télé intelligente, avec une caméra devant, tu sais pas où ça peut se rendre.*[110]

Nous avons également évoqué avec le réalisateur l'aspect de la sensibilisation : avait-il comme but que les gens changent leurs habitudes, qu'ils évitent les comportements à risque dans le cyberespace ? « Oui, l'idée, nous a-t-il dit, c'était de vulgariser ça et que les gens partent avec une information de ça, et après, c'est à eux de décider : est-ce qu'ils veulent protéger leur vie privée et prendre des précautions ou considérer que de toute façon tout se sait déjà à leur sujet ?[111] ».

---

[109] Nacer, S. (2017, 6 juin). Entrevue avec Bachir Bensaddek sur la série documentaire *Hackers*, Montréal, QC.
[110] *Ibid.*
[111] *Ibid.*

Finalement, nous avons questionné le réalisateur afin de confirmer si les messages portés par la série avaient un caractère éducatif, voici sa réponse :

> *Un côté éducatif, très certainement. On voulait sensibiliser les gens à cette réalité-là et les laisser avec l'information. Et puis, peut-être que c'est à eux ensuite de creuser et de fouiller, mais leur ramener des données comme VPN, cryptage, hameçonnage, vie numérique, vie virtuelle, tout ça, ça te fait dire ok finalement ça se fait pas tout seul : toi, tu entres ton nom, ta carte de crédit et ton mot de passe, et hop, super, tu peux utiliser Google, Amazon, Apple, Ticket Master. Seulement, t'as un profil là et il faut que tu réfléchisses à où ça va.*[112]

Nous comprenons donc que c'est à travers le loisir, l'intrigue et la peur que le réalisateur de la série a construit ses messages, et ce, en suscitant de l'émotion, qui demeure l'élément central de la narration. L'aspect éducatif de la série se concrétiserait selon lui dans le fait qu'elle amènerait à de nouvelles pratiques et à des comportements plus sécuritaires dans le cyberespace.

Cette entrevue avec le réalisateur nous a permis de savoir quels étaient les objectifs communicationnels de la série *Hackers*. Nous tenterons maintenant de déterminer, à partir des témoignages des téléspectateurs que nous avons sélectionnés, si ces objectifs ont été atteints. Car la question qui se pose est la suivante : est-ce que cette série documentaire provoque vraiment une prise de conscience ?

4.2 Présentation de notre échantillon

Notre échantillon se compose de sept participants : 3 femmes, et 4 hommes; il est donc majoritairement masculin. Parmi les 4 hommes, 3 sont âgés de 25 à 54 ans; ils

---

[112] *Ibid.*

représentent donc l'auditoire cible de la série du point de vue de l'âge. Parmi les trois femmes, l'une est âgée de 47 ans, une autre de 67 ans et la troisième est âgée de 17 ans. Tous nos répondants sont établis à Montréal, et les entrevues ont été réalisées près de leur lieux de résidence, afin d'instaurer un climat de confiance, d'autant plus qu'ils ont eux-mêmes choisi le lieu de l'entrevue. En ce qui concerne leur scolarité, une répondante était en cinquième secondaire, un répondant était étudiant au premier cycle en sciences humaines et sociales, deux répondants avaient complété un baccalauréat et trois possédaient une maîtrise. Leurs occupations étaient les suivantes : infirmière à la retraite, informaticien, rédactrice, chargé de communication, musicien professionnel et finalement deux étudiants, de niveau secondaire et universitaire. Les profils de ces répondants présentent donc une certaine hétérogénéité socioéconomique, ce qui nous apparaît pertinent pour notre étude. Mentionnons que le réalisateur de la série fait partie des 25-54 ans et qu'il réside à Montréal.

Afin de dissiper le doute quant à la capacité de la série de s'adresser à un auditoire plus vaste que celui utilisé dans notre recherche, nous avons demandé à nos répondants s'ils avaient ressenti une difficulté, une quelconque gêne ou un ennui lors du visionnage de la série. Les réponses ont été unanimes : « J'ai trouvé que c'était assez simple, on comprend ce qu'ils disent », « Ils vulgarisent vraiment des informations qui peuvent paraître compliquées, finalement ça devient simple », « J'ai aimé la simplicité avec laquelle c'est raconté », « Je pensais au départ que ce serait difficile, mais j'ai trouvé ça simple et très intéressant ».

En ce qui concerne l'intérêt pour la série, nous les avons questionnés sur le temps de visionnage : « Je les ai vus d'un seul coup », « Je les ai vus en une soirée avec mon mari, et c'était comme voir un film », « J'avais prévu de les voir en deux fois, mais je les ai vus d'un coup, ça passait vraiment vite ». Ils ont ajouté : « Ça m'intéressait de

savoir la suite, et je voulais pas attendre », « C'était pas long, donc j'ai préféré enchaîner », « J'étais curieuse d'en savoir plus ».

Notons cependant que le[113] répondant n° 2 est le seul à avoir manifesté une légère difficulté à assimiler certaines informations contenues dans la série: « Il y a des choses que j'avais jamais entendues ». Lorsque nous lui avons demandé d'expliquer sa réponse, il a parlé de son manque de familiarité avec la technologie : « C'est sûr que j'utilise pas autant Internet que mes enfants ou mes petits-enfants ».

Rappelons ici que nous avons questionné le réalisateur sur l'auditoire cible de sa série, en lui rapportant les commentaires de nos participants.

> *C'est sûr, Explora a son public, et ça, tu peux pas le réinventer mais moi, je l'ai fait pour que n'importe qui le comprenne. Au départ, je me disais pas : je m'adresse à des gens qui sont d'un milieu aisé et qui ont de quoi s'acheter un iPhone ou autre chose. Je suis parti du principe qu'il y a beaucoup de gens qui sont connectés, même quand ils n'ont pas beaucoup de moyens. Tu sais, les gens vont peut-être s'endetter pour s'acheter un téléphone, pour avoir du temps d'antenne, donc voilà : pour moi c'était vraiment le grand public.*[114]

Sa réponse confirme que l'auditoire ciblé par le documentaire ne se limite pas à l'auditoire cible de la chaîne ICI Explora. De plus, les réponses de nos répondants tendent à confirmer qu'ils n'ont pas ressenti d'ennui ou de difficultés majeures à comprendre les thématiques abordées. Nous considérons donc qu'ils ont porté un véritable intérêt à la série *Hackers,* et que leurs réponses sont dès lors pertinentes pour notre recherche.

---

[113] Afin d'alléger le texte, nous utiliserons le masculin pour désigner nos répondants dans la présentation de notre analyse.
[114] *Ibid.*

Tableau 4.1. Présentation de notre échantillon

Le tableau suivant présente notre échantillon et les caractéristiques démographiques et économiques propres à chaque répondant. Ce tableau permet également une lecture simplifiée des résultats que nous allons présenter dans les prochains chapitres. Nous avons associé chaque répondant à un numéro.

Répondant	sexe	âge	occupation	niveau d'étude	lieu de résidence
1	M	22	étudiant	baccalauréat en cours	Montréal
2	F	67	infirmière à la retraite	baccalauréat	Montréal
3	F	47	rédactrice	maîtrise	Montréal
4	M	37	chargé de communication	baccalauréat	Montréal
5	M	42	informaticien	maîtrise	Montréal
6	F	17	étudiante	secondaire	Montréal
7	M	33	pianiste professionnel	maîtrise	Montréal

4.3 Accès à Internet et rapport à la technologie

Les informations collectées lors de nos entrevues semi-directives nous ont permis de confirmer quels types d'usagers étaient représentés par nos répondants, et quel était leur rapport à la technologie. L'analyse de leurs réponses nous a donc permis de mettre en lumière une certaine variabilité des usages qui concordait sans surprise avec les caractéristiques propres à chaque profil. Notons ici que les éléments de réponse considérés dans cette première analyse concernaient principalement les deux premiers épisodes, soit celui traitant du vol d'identité et celui traitant du viol virtuel et de la cyberintimidation.

Tous nos répondants ont affirmé avoir accès à Internet et tous possédaient un cellulaire « intelligent ». Quatre d'entre eux ont affirmé utiliser leur cellulaire de manière très fréquente et que c'était principalement pour accéder à Internet. « Je passe beaucoup de temps à l'université et mon cell est généralement toujours connecté sur notre réseau » (répondant n° 1). « Je reçois dessus des notifications sur les nouvelles, j'ai besoin de savoir ce qui se passe dans ma job » (n° 4).

> *Généralement mes clients me contactent par courriel. Je reçois les mandats, ou les informations sur ce qui va pas, par exemple si le système bloque à quelque part, ça me permet de commencer à travailler sur le cas en lisant les infos qu'ils m'envoient d'où je me trouve. (n° 5)*

« Je suis toujours connecté, même si en cours on n'est pas censés le faire... (rire) » (n° 6). Un des répondants a affirmé utiliser le cellulaire principalement pour passer des appels mais sur des applications mobiles qui nécessitent donc une connexion :

> *J'utilise ce téléphone offert par ma fille. Je sais que je peux me connecter sur Skype pour parler également à ma sœur qui vit à l'étranger. D'ailleurs, je dois avouer que j'ai tellement économisé d'argent depuis*

> *que cela existe, avant on devait attendre au moins deux semaines pour pouvoir se parler (n° 2).*

Les deux autres répondants ont dit utiliser peu leur cellulaire pour accéder à Internet. « J'ai Internet sur mon cellulaire mais je l'utilise généralement pour appeler mes enfants, par exemple le mardi et le jeudi, lorsque je dois récupérer ma fille du sport, cela m'évite de devoir l'attendre au parking » (n° 3). « Mon cell., c'est plus pour être joint, même si j'ai un forfait avec data » (n° 7).

Les habitudes de nos répondants illustrent bien le taux de pénétration d'Internet dans les foyers canadiens. « Les chiffres relatifs à l'utilisation du Net sont impressionnants. En janvier 2017, 33 millions sur les 36 millions de la population totale sont des internautes, ce qui représente 91 % de la population[115] ». Notons que le fait que tous nos participants résident à Montréal explique sans doute le fait qu'ils utilisent Internet dans une proportion encore plus forte que la population en général. On peut faire la même réflexion en ce qui concerne l'usage du téléphone intelligent.

> *Comme partout ailleurs dans le monde, l'usage du téléphone s'est fortement répandu. À tel point que le Canada se situe au-dessus de l'échelle, avec 82 % de la population canadienne qui utilise un mobile. 73 % de la population possèdent des téléphones intelligents.*[116]

En ce qui concerne l'accès à Internet et la possession d'un appareil cellulaire intelligent, nos résultats confirment les tendances. Nous demeurons cependant conscients que même si nos résultats sont validés par les statistiques, nous ne pouvons les généraliser, car la taille de notre échantillon limite la portée de nos

---

[115] KAP Tactiques numériques. (2017). « Les chiffres du numérique au Canada en 2017 ». Récupéré de http://www.kap-numerique.com/chiffres-numerique-canada-2017/

[116] *Ibid.*

résultats. Ils demeurent néanmoins pertinents aux fins de notre recherche, car ils nous permettent de comprendre comment nos répondants « consomment » Internet.

4.4 Réception des messages de la série par nos répondants

Comme nous avons choisi de nous inspirer du type d'analyse développé par Stuart Hall – basée sur la notion de codage/décodage – nous tenterons de déterminer au sein de quelles positions « hypothétiques » de réception s'inscrivent les résultats de nos entrevues. Nous citerons à cette fin des extraits (les plus représentatifs) des sept verbatim de nos entrevues.

Une première lecture de nos résultats a permis de mettre en lumière l'existence d'une concordance entre certains messages produits par le réalisateur et la réception de ces dits messages. Cette concordance s'est manifestée en premier lieu dans les réponses de nos répondants. Le premier et le second épisodes traitant, selon le réalisateur lui-même, des conséquences directes du *hacking* sur les individus, l'ensemble de nos répondants a perçu clairement les messages principaux et en a mentionné les éléments clés : « piratage », « hacker », « vol », « usurpation d'identité », « surveillance », « réseau non sécurisé », « réseau public », « Wi-Fi », « cartes ou comptes bancaires ». Voici quelques extraits des réponses relatives au premier épisode.

« Ça montre que le vol et l'usurpation d'identité, ça peut se faire simplement, et on peut même voler ton compte bancaire par le biais du piratage informatique, entre autres en simulant un Wi-Fi gratuit » (répondant n° 1). « Avec des informations que l'on peut collecter des ordinateurs ou des cellulaires d'individus, on peut usurper leur identité et disposer de tous les privilèges qui y sont associés (carte de crédit, passeport, comptes bancaires…) » (n° 5). « C'est facile pour les pirates d'accéder aux informations d'une personne qui n'as pas pris de mesures pour sécuriser ses

informations, par exemple sur le Wi-Fi public » (n° 6). « Ça parle du vol d'identité, et du risque de voler des informations, de violer ta vie privée… des informations très importantes, des informations clés, des cartes bancaires… etc. On peut scanner des puces. On n'est jamais assez protégés, que ce soit dans les magasins, ou même à distance, le risque est très présent, surtout si ta connexion est non sécurisée. » (n° 4)

Nous avons pu également relever une certaine similitude dans les réponses de nos répondants lorsque nous leur avons demandé ce qu'ils avaient retenu de ce premier épisode et quelles étaient les meilleures pratiques à favoriser afin d'éviter de se faire voler son identité :

« Il ne faut pas se connecter n'importe où et être vigilants quand on utilise nos équipements. » (n° 5); « Il faut faire très attention aux informations mises sur ses appareils intelligents et ne plus me connecter aux réseaux de connexion publics. » (n° 6); « Éviter de se connecter souvent et dans les cafés, les parcs, enfin là où c'est gratuit. De toute manière, généralement, la gratuité n'apporte rien de bon. » (n° 2); « Éviter les réseaux sans fil publics, surtout pour y réaliser des transactions bancaires. » (n° 7); « Qu'il faut se servir de son jugement, mais qu'on risque tous d'être victimes d'un pirate éventuellement. » (n° 3)

De manière générale, nos répondants ont affirmé avoir été surpris par les informations contenues dans ce premier épisode : « Oui, j'ignorais le danger et la facilité que les *hackers* ont pour voler ces informations. » (n° 6); « Oui, un peu, bien sûr que ça nous met en garde. C'est effrayant un peu parce qu'on a peur d'être victime un jour. » (n° 3); « Un peu surpris par l'ampleur des possibilités qui s'offrent aux pirates. » (n° 1); « Pas vraiment, il y a tant de lecture à ce sujet, par contre voir la facilité avec laquelle on peut soutirer de l'information reste étonnant. » (n° 5); « Un peu, parce que les conséquences de ces piratages peuvent être désastreuses pour notre intimité et surtout qu'on peut être piratés même si l'on prend nos précautions. » (n° 4); « C'est

effrayant, toute cette technologie. » (n° 2). « Je pensais en savoir assez, mais ça me choque toujours autant. » (n° 7).

Le réalisateur de la série, comme nous l'avons dit, voulait, dans son axe communicationnel, susciter chez l'audience de la série un certain sentiment de peur, dans l'intention de provoquer un changement de comportement. Les commentaires de nos répondants démontrent en effet qu'ils ont bien ressenti ce sentiment de peur, qui demeure un élément central de la série. Les commentaires au sujet du second épisode, qui traite du viol virtuel et de la cyberintimidation, présentent une certaine similarité dans la réception des messages. Notons, pour cet épisode, que ce qui a majoritairement retenu l'attention de nos répondants n'était pas tant le fait que les *hackers* ciblaient des célébrités (« Parce qu'on sait que quand on est une célébrité, y'a toujours le risque, on le sait déjà, on est plus étonné quand c'est des personnes ordinaires. » [n° 4]), mais plutôt la facilité avec laquelle ces *hackers* peuvent prendre le contrôle et pirater des comptes personnels : « Les réseaux sociaux peuvent être utilisés pour de l'intimidation et peuvent détruire la vie de certains individus » (n° 3); « Nous ne sommes jamais à l'abri d'un vol de notre intimité. » (n° 4); « Nos données personnelles mises sur Internet sont susceptibles d'être utilisées contre nous… nos photos et vidéos sont facilement accessibles pour les pirates. » (n° 1); « J'ai raison de m'inquiéter, les jeunes sont fous, ils mettent toute leur vie sur Internet et après, ils se plaignent de pas avoir de vie privée. Tout le monde veut être une star aujourd'hui. Je pense que moins vous en mettez, mieux vous vous portez » (n° 2).

Ce qui est également ressorti de notre analyse est que l'ensemble de nos répondants ont retenu l'importance de sécuriser leurs mots de passe. « Faut donner aucun mot de passe à qui que ce soit et faut avoir des *backups* pour ses comptes » (n° 6); « Peut-être crypter le mot de passe, le changer souvent, heu... Faut se déconnecter à chaque fois, se déconnecter sans enregistrer le mot de passe à chaque fois » (n° 4); « Protéger ses équipements par des mots de passe forts et les modifier souvent, ne pas mettre sur les

réseaux des activités qui peuvent révéler des informations pouvant être exploitées par des personnes malintentionnées » (n° 5); « Donner moins d'informations personnelles lors d'inscriptions sur Internet et éviter des mots de passe trop simples. Faut aussi éviter de stocker des documents importants sur le *cloud,* surtout pour ce qui est de documents personnels tels que le passeport » (n° 1).

Les commentaires relatifs aux autres épisodes ont également démontré une grande concordance en ce qui concerne la perception des messages. De manière générale, ce qui est ressorti des réponses de nos répondants au sujet de l'épisode 3 (Les États), c'est la compréhension de ce que signifie le terme « cyberguerre », qui est cité dans l'ensemble des réponses. Cependant il apparaît que, même si nos répondants ont semblé avoir intégré le concept sur le plan théorique, la majorité d'entre eux n'a pas été capable de développer davantage sur le sujet ou de faire un lien direct avec la prolifération des cyberattaques. Ainsi, à la question de savoir si une cyberguerre était selon eux en cours, leurs réponses ont été plutôt négatives : « Non, mais une pourrait certainement éclater d'un jour à l'autre » (n° 1); « Je ne pense pas » (n° 7); « Non! » (n° 6). Un de nos répondants s'est cependant démarqué, et sa réponse à la même question témoignait d'une certaine connaissance du sujet : « Absolument, et depuis longtemps. L'un des effets visibles est le vol de l'information technologique (inventions, brevets...). L'information a toujours été au centre des guerres entre nations. Cela est encore plus vrai aujourd'hui » (n° 5).

Les réponses aux questions relatives à l'épisode 4 (Les entreprises) ont révélé que majoritairement nos répondants se doutaient de l'existence de risques au sein des grandes entreprises et institutions telles que les banques. Cependant, ils n'avaient généralement pas ou peu conscience du niveau élevé de cette menace, notamment celles portant sur l'accessibilité et le vol d'informations personnelles. On pouvait ainsi déceler une certaine surprise face aux informations données dans cet épisode : « On peut finalement pirater une entreprise comme une personne ...c'est pareil. Ça

m'a fait penser à l'épisode 2, mais cette fois-ci c'était une entreprise, pas une personne. » (n° 4) ; « C'est plus facile qu'on pense d'accéder aux informations personnelles d'une personne » (n° 6); « Rien ni personne n'est à l'abri finalement » (n° 2). Ici encore, les réponses du répondant n° 5 étaient plus nuancées. Rappelons que ce dernier travaille dans le domaine de l'informatique. Il semblait moins surpris par ce qu'il avait appris en visionnant l'épisode : « Ce n'est pas surprenant... je pense qu'il y a de plus en plus de conscience relativement à la sécurité. Mais il y a de plus en plus d'attaques qui se font parce que parfois c'est plus facile pour tenter des actions criminelles bien à l'abri des regards ». Nous avons cependant relevé un fait intéressant dans ses réponses. En effet, même s'il semblait avoir une grande connaissance des technologies de l'information, il a pourtant déclaré qu'après avoir pris connaissance de cet épisode, il envisageait de changer certaines habitudes : « C'est important de mieux comprendre les risques de sécurité, de mettre en place des contrôles de sécurité selon des standards reconnus et contrôler leur exécution ».

Nos répondants ont admis ne pas être familiers avec le concept d'*hacktivisme,* traité dans le dernier épisode. Les commentaires à ce sujet indiquent une perception assez disparate de ce phénomène. Il semble difficile pour certains de nos répondants de ne pas condamner les méthodes des *hacktivistes*, même si ce cinquième épisode tentait de démontrer qu'il y avait deux profils ayant des intentions opposées. « C'est des gens qui connaissent le système et qui s'en servent ... Ils disaient qu'il y a des gens qui font ça, enfin qui disent faire ça pour protéger. Je ne sais pas trop : quand quelqu'un peut rentrer chez vous quand il veut, est-ce que vous pouvez lui faire vraiment confiance ?... » (n° 2); « Comment contrôler ce qu'ils font ?... Comment s'assurer que quelqu'un n'en profite pas pour ses propres intérêts au détriment des autres ? » (n° 7). D'autres semblaient cautionner les méthodes des *hacktivistes* : « La fin justifie les moyens. La procédure peut être mauvaise mais, tant qu'il y a un bon résultat, j'estime que cette procédure était utile. » (n° 1). Finalement, certaines réponses indiquaient une certaine compréhension de l'utilité de l'*hacktivisme* tout en

condamnant le *hacking :* « Malgré le bon côté des *hacktivistes,* ils peuvent causer beaucoup de dommages » (n° 6); « Sans éthique, l'hacktivisme pourrait s'avérer être une arme aussi destructrice que les vraies armes » (n° 5).

Nos entrevues nous ont également permis de sonder nos répondants afin de savoir s'ils comptaient changer leurs habitudes à la suite du visionnage de la série. Ici encore, il y a en général une homogénéité des réponses. Cependant, nous avons noté que, selon les caractéristiques de leurs profils, les participants manifestaient un niveau varié de prise de conscience au sujet des comportements à risque. Ainsi, en ce qui concerne les répondants faisant un usage régulier ou fréquent d'Internet, nous avons remarqué qu'ils répondaient tous « oui » à la question de savoir s'ils allaient changer leurs habitudes. (n^{os} 1, 6 ,4). Pour ceux qui faisaient un usage moins fréquent ou qui considéraient avoir un comportement plus sécuritaire, les réponses indiquaient plutôt qu'ils allaient tenter d'être davantage vigilants (n^{os} 2, 3, 5,7). Finalement, l'ensemble de nos répondants ont affirmé qu'ils allaient communiquer autour d'eux sur ce qu'ils avaient appris.

4.4.1 La « position de réception » des téléspectateurs de *Hackers*

Nous nous questionnerons maintenant sur la « position de réception » de nos répondants. Rappelons que nous adoptons pour ce faire l'analyse proposée par Stuart Hall, qui vise à évaluer la concordance entre les messages que le producteur de la communication a voulu véhiculer au moment du « codage » de ces messages et la réception de ces messages dans le processus de « décodage ».

Les résultats des entrevues avec nos répondants nous révèlent la manière dont ils ont lu et interprété les messages portés par la série documentaire. D'après Hall, la « concordance » des résultats avec les propos du réalisateur démontrerait une

« communication parfaitement transparente ». Ce type de communication supposerait que le récepteur du message fait partie de la « position dominante-hégémonique ». Ce type de réception supposerait que le « téléspectateur opère au sein du code dominant[117] », et qu'il n'a présenté aucune forme de résistance aux messages qui lui ont été présentés. On peut dès lors conclure qu'il a adhéré aux valeurs et contenus de ces messages sans aucune distorsion sur le plan du « sens ».

D'après les résultats de notre recherche, on peut affirmer que nos répondants ont de manière générale bien reçu les messages transmis par le réalisateur et qu'ils y ont adhéré sans tenter de les interpréter différemment. Cela indique, selon Hall, l'existence d'une « relation d'équivalence » entre les positions des « personnifications[118] » du « codeur-producteur[119] » et du « décodeur-récepteur[120] ». Nos répondants et le réalisateur opèrent donc au sein de « cadres de connaissances » communs. Nous pensons que cela s'explique par le fait qu'ils vivent dans le même environnement, et partagent donc plusieurs référents culturels et sociaux. Nous pensons également que cela favorise, sur le plan du traitement de l'information, l'adhésion commune à certains messages et valeurs.

Nous avons indiqué précédemment que notre échantillon se composait de plusieurs profils d'usagers : certains répondants ont indiqué utiliser Internet de manière assez fréquente, d'autres de manière occasionnelle. Nos résultats démontrent pourtant que les informations transmises par la série ont interpellé l'ensemble de nos répondants. Nous pensons que cela s'explique par le fait que, même si cette série met en évidence

---

[117] Hall, Stuart, Albaret, Michèle. et Gamberini, Marie-Christine. (1994) « Codage/décodage », [chapitre de livre] In: *Réseaux,* volume 12, n° 68, 1994. Les théories de la réception. (p. 27-39). Récupéré de *www.persee.fr/doc/reso_0751-7971_1994_num_12_68_2618*

[118] *Ibid.*

[119] *Ibid.*

[120] *Ibid.*

une certaine corrélation entre le type d'usager et le niveau de risque, elle révèle néanmoins que toute personne présente dans le cyberespace s'expose au *hacking.*

Si notre analyse nous incite à attribuer à nos récepteurs ce que Hall appelle la « position dominante-hégémonique » à cause de leur adhérence générale aux messages des producteurs de la série, nous pensons qu'il y a, dans certaines de leurs réponses, des éléments de « position négociée ». Selon Hall, ce type de réception s'explique par le fait que « les codes négociés fonctionnent à travers ce que l'on pourrait appeler des logiques situées, ou particulières[121] ». Ainsi, au moment du processus de *décodage,* le téléspectateur « accorde la position privilégiée aux définitions dominantes des événements, tout en réservant aux "conditions locales", à ses propres positions plus corporatistes, le droit d'effectuer une application plus négociée[122] ». Nous avons pu observer cela au sein de notre auditoire dans les réponses relatives aux troisième et cinquième chapitres. Nos répondants ont ainsi manifesté une certaine adhésion aux messages véhiculés dans ces épisodes tout en « négociant » cependant la finalité de ces messages. Ainsi, à l'exception de l'informaticien, tous nos répondants ont affirmé qu'aucune cyberguerre n'était en cours. L'épisode soulignait pourtant l'existence de plusieurs conflits majeurs entre les États, et l'analyse des entrevues mettait en évidence une bonne compréhension du phénomène lui-même. Nous pensons que cette forme d'exclusion s'explique par le fait que la guerre est associée dans l'imaginaire collectif à la violence et au chaos; de ce fait, en l'absence de ces paramètres, il était difficile pour nos répondants d'affirmer qu'une cyberguerre était déjà en cours. Il apparaît ici que la cyberguerre est un concept qui n'est pas encore intégré dans le cadre de référence de nos répondants. Ils ont saisi les messages mais les ont adaptés à leur « conditions locales [123]». Notre

---

[121] *Ibid.*
[122] *Ibid.*
[123] *Ibid.*

informaticien étant plus familier avec les enjeux de cybercriminalité, il avait donc déjà intégré ce concept. Sa réceptivité en tant que « décodeur-récepteur[124] », résulte de connaissances communes et partagées avec le « codeur-producteur [125] » des messages, à savoir le réalisateur. La *position négociée* peut également être observée dans la réception du dernier épisode de la série. Le même répondant est le seul à démontrer une acceptation totale de la réalité de l'*hacktivisme*. Les réponses des autres répondants témoignent du fait qu'ils sont capables de distinguer les deux profils d'hacktivistes présentés dans cet épisode, mais qu'ils condamnent néanmoins leurs méthodes. Nous pensons que les phénomènes traités dans cet épisode demeurent encore très peu connus du grand public. De ce fait, lors du processus de décodage des messages, nos répondants ont fait appel à leurs propres cadres de référence pour désigner ce qui était légal ou pas, « négociant » ainsi les messages portés par cet épisode.

Finalement, nous n'avons relevé dans les réponses de nos répondants aucune forme d'opposition radicale aux messages de la série, ce qui nous pousse à exclure ce que Hall appelle la « position oppositionnelle ».

---

[124] *Ibid.*
[125] *Ibid.*

CONCLUSION

À l'heure où les communications politiques et institutionnelles, de même que les normes sociales, semblent s'accorder unanimement sur l'importance d'Internet, notre rôle de chercheure nous pousse à nous interroger sur le rôle des communications dans la sensibilisation aux enjeux sécuritaires liés à cette « hyperconnectivité ». Notre recherche, qui s'inscrit dans l'analyse de contenu d'un média selon une codification inspirée de Stuart Hall (1973), a pour objectif de comprendre comment la série documentaire *Hackers*, diffusée en 2016 sur la chaîne ICI Explora, tente de vulgariser, sensibiliser et également éduquer sur les enjeux liés à la cybercriminalité et aux identités numériques. Une étude de la littérature existante nous a orientés vers les travaux de trois chercheurs principaux, dont les recherches ont balisé notre travail. Nous nous sommes ainsi intéressée aux travaux de Pierre-Léonard Harvey (1995) afin de comprendre le comportement des usagers dans le cyberespace et de les inscrire dans une perspective de recherche en communication. Les travaux de Stuart Hall nous ont orientés vers le choix d'une méthodologie pertinente, offrant les outils nécessaires à l'analyse de la réception de messages médiatiques. Finalement, les travaux d'Adam Segal (1996) nous ont offert l'encadrement théorique nécessaire afin d'aborder les phénomènes liés à la cybersécurité traités par la série documentaire *Hackers*.

Afin de répondre à notre question de recherche, nous avons donc mis en place une recherche axée sur une méthodologie ancrée dans le champ des communications, et s'inscrivant dans le paradigme de la recherche systémique. Cette méthodologie a eu pour but de nous permettre de faire une lecture pertinente des diverses données collectées sur le terrain.

Nous avons donc réalisé cette recherche en deux étapes. La première consistait à comprendre le processus d'encodage des messages médiatiques de la série documentaire. Pour cela, nous avons mené une entrevue avec le réalisateur, qui nous a permis d'explorer le contenu de chaque épisode et d'en préciser les messages clés. Cette première étape, qui s'inscrit dans l'analyse du « codage du signe télévisuel », nous a également permis de comprendre l'objectif communicationnel porté par chaque épisode, et les éléments déterminants dans la structure de ces messages. En marge de cette première étape nous avons pu distinguer nos premiers éléments de réponses à notre question de recherche. En effet, l'analyse de contenu de chaque épisode ainsi que l'entrevue du réalisateur a permis de mettre en lumière les structures communicationnelles mises en place pour que la série documentaire *Hackers* puisse communiquer, sensibiliser et éduquer sur les grands enjeux touchant la cybercriminalité et les identités numériques. Nous avions donc assez d'éléments structurants pour mettre en place nos entrevues individuelles, et sommes donc passée à la seconde phase de notre méthodologie, à savoir l'analyse de la réception de la série *Hackers* ou, en d'autres termes, du « décodage du signe télévisuel ». Nous avons ainsi sélectionné plusieurs répondants représentant différents profils d'usagers d'Internet. Nous avons mis en ligne notre appel à candidature, et avons par la suite sélectionné nos participants d'après les critères préalablement établis. Nous leur avons envoyé les liens des épisodes de la série documentaire afin de leur permettre de les visionner dans un cadre « naturel », nous basant ainsi sur l'approche ethnographique du chercheur David Morley (1993). Chacun des cinq épisodes de 30 minutes explorait un thème spécifique au piratage informatique : le vol d'identité, le viol virtuel et la cyberintimidation, le cyberterrorisme, les attaques informatiques à l'endroit des entreprises, et les opérations menées par les « hacktivistes ». Nous avons par la suite réalisé nos sept entretiens individuels, d'une durée de 40 à 60 minutes chacun : six furent réalisés en personne, et un fut réalisé à distance à l'aide du logiciel de vidéoconférence Skype. Les résultats ainsi obtenus ont été transcrits puis analysés

selon la méthode de l'analyse de contenu catégorielle proposée par Laurence Bardin (1996).

Une première analyse des résultats a eu pour but de déterminer les messages clés perçus par nos répondants afin de comprendre si les objectifs communicationnels du réalisateur se concrétisaient au sein de notre audience. Cette étape a permis de mettre en lumière l'existence d'un fort degré d'équivalence entre les messages véhiculés par le réalisateur et leurs interprétations de la part de l'audience. Cette concordance de la réception des messages avec l'intention des producteurs nous a poussée à inscrire principalement la réception de la série documentaire au sein de la *position dominante-hégémonique*. Cette dernière se cristallise au sein d'une audience qui partage des cadres de référence communs avec les producteurs de messages. Dans le processus de décodage, cela entraîne une concordance en ce qui concerne l'interprétation; il en résulte une communication dite « transparente ». En nous basant sur l'approche de Hall, nous avons pu relever la présence d'une seconde « position de réception » des messages médiatiques au sein de notre audience. Il s'agit de la *position négociée*, qui s'est manifestée principalement dans les réponses relatives aux thématiques portant sur des enjeux plus éloignés des réalités partagées par la majorité de nos répondants. En effet, sur les enjeux relatifs au cyberterrorisme et à l'hacktivisme traités dans les troisième et cinquième épisodes, à l'exception de notre répondant travaillant dans le domaine de l'informatique, nous avons pu relever une certaine « distorsion » dans la lecture des messages, comparativement aux autres épisodes. Selon Hall, le degré de « symétrie » dans les échanges communicationnels témoigne de l'adhésion aux messages. De ce fait, nos résultats témoignent, de la part de nos répondants, de leur niveau de connaissance des sujets traités : ils adhèrent aux messages ou les adaptent selon leurs cadres de référence. Plus ils sont informés sur les sujets traités, plus leur adhésion aux messages véhiculés est forte. Cela explique pourquoi l'auditoire a pu assimiler de manière claire les enjeux touchant ses habitudes de consommation, et la protection de ses données. Cependant, quand il s'est agi des enjeux relatifs à la

sécurité des États, ou encore des actions menées par les *hacktivistes,* l'adhésion aux messages aurait nécessité une meilleure connaissance de ces questions. Notre analyse a toutefois démontré que nos répondants n'ont pas rejeté les messages, mais les ont « négociés » pour que leur interprétation concorde avec leurs cadres de référence.

Nos résultats nous ont également permis de relever au sein de notre auditoire une volonté de changer leurs comportements dans le cyberespace. Et, même si ces comportements diffèrent selon les types d'usagers, nous pensons que cette volonté de changement résulte du fait que la série documentaire a su provoquer une réelle prise de conscience. Nous avons d'ailleurs démontré que le réalisateur avait fait appel à l'*intrigue* comme élément structurant de son scénario. Cela a permis de sensibiliser l'auditoire aux différents risques auxquels ils s'exposaient dans le cyberespace, car « l'émotion » constitue l'élément clé dans la narration documentaire. Ainsi, en réponse à notre question de recherche, nous croyons que la prise de conscience et la volonté de changement confirment la réussite de l'intention d'informer et d'éduquer de la série documentaire. La narration construite autour de l'intrigue vient concrétiser les objectifs communicationnels du producteur en suscitant l'intérêt de l'auditoire. L'émotion renforce l'absorption des messages transmis, et les cadres de référence influencent le type de réception.

Nous avons conscience que notre recherche, bien qu'elle s'appuie sur une méthodologie et des références théoriques pertinentes, comporte certaines limites. Tout d'abord, la taille réduite de notre échantillon limite naturellement la portée des conclusions de notre recherche et les possibilités de généralisation à l'ensemble du public de la série. Notre audience est constituée de membres sélectionnés sur la base de critères que nous avons mis en place pour le bien de la recherche : de ce fait, il ne s'agit pas d'un échantillon représentatif du « vrai public » de la série. De plus, comme dans toute recherche s'inscrivant dans l'étude de la réception de messages, la méthodologie choisie influence les résultats; nous pensons ainsi que notre

méthodologie nous a permis de mettre en lumière « des perceptions de la réalité, et non la réalité en soi » (Dépelteau, 1998, p.313). Nous avons, en effet, analysé un discours sur l'expérience plutôt que l'expérience elle-même, ce qui d'une certaine manière influe sur les résultats. Également, le fait d'avoir construit nos entrevues à partir de notre propre lecture de la série et d'avoir adopté une analyse qualitative implique une interprétation subjective, qui doit être considérée dans la prise en compte des résultats. Finalement, notre conclusion relative à la prise de conscience de notre auditoire et son éventuel changement de comportements repose sur son propre discours. Nous ne pouvons confirmer avec certitude que ces changements auront réellement lieu, car cela nécessiterait de mettre en place une méthodologie d'observation comportementale sur une plus longue période de temps.

Étant donné ces limites, nous recommandons que lors de futurs projets de recherche, la taille de l'échantillon, le type d'observation mais également la durée de la recherche soient éventuellement ajustés afin d'optimiser les résultats. Nous pensons tout de même que notre travail demeure pertinent et nécessaire pour la recherche en communication. En effet, à l'heure où le développement technologique guide nos pratiques tant de socialisation que de communication, il apparaît primordial pour les chercheurs d'offrir des pistes de réflexion sur l'évolution des interactions sociales, mais également sur l'évolution des formes de communication et des divers enjeux sécuritaires que cela implique. Nous espérons ainsi poser ici les jalons d'une première ébauche de recherche, qui pourrait servir de point de départ à diverses autres réflexions et analyses sur le rôle des communications dans l'éducation et la sensibilisation aux enjeux relatifs à la cybersécurité.

Tel que souligné en introduction de ce travail de recherche, l'accès à Internet demeure un enjeu prioritaire dans notre société, et ce, même si le nombre de cyberattaques croît considérablement. Récemment, le gouvernement provincial a conjointement annoncé avec son homologue fédéral un investissement de 290

millions de dollars « pour brancher en région 100 000 foyers et entreprises québécoises à Internet haute vitesse d'ici cinq ans »[126]. Nous apprenions le lendemain que « l'entreprise de transport automobile Uber aurait été victime d'un piratage massif, dans le cadre duquel les informations personnelles de 57 millions de personnes, chauffeurs comme clients, auraient été dérobées »[127]. L'éducation et la sensibilisation, tant du public que des professionnels, mais également la compréhension des enjeux touchant la protection des données et la sécurité des usagers nous poussent à considérer que les communications auront dans les années à venir un rôle important à jouer. Nous devrons en tant que chercheurs trouver des pistes de solution afin d'harmoniser les pratiques dans un contexte de développement constant des technologies de l'information.

---

[126] Radio-Canada. (2017, 20 novembre). 290 millions pour offrir Internet haute vitesse à 100 000 foyers en région. *Radio-Canada.ca*. Récupéré de http://ici.radio-canada.ca/nouvelle/1068198/quebec-ottawa-internet-haute-vitesse-region-investissement

[127] Radio-Canada. (2017, 21 novembre). Piratage massif chez Uber : les données de 57 millions de personnes dérobées. *Radio-Canada.ca*. Récupéré de *http://ici.radio-canada.ca/nouvelle/1068600/transport-uber-faits-divers-piratage-donnees-personnelles*

ANNEXE A

ENTREVUE DU RÉALISATEUR – 6 JUIN 2017

Question 1- Bonjour Bachir alors pour commencer peux-tu me parler un peu de la série, et de son objectif

Une des critiques qu'un collègue m'a faite qui a regardé la série, qui était intéressée c'était qu'on ne proposait pas de solutions à la fin, on avait toujours un récapitulatif à la fin avec Mathieu notre animateur qui rencontrait les victimes, les gens comme ça qui disait …ah voilà vous auriez pu faire si vous auriez pu faire ça mais lui il aurait aimé quelque chose d'un peu plus …tu sais plus scolaire, comme un tableau en disant ne faites pas ci ne faites pas ça, si ça vous arrive faite ci faite ça et voilà, c'était pas dans le format qu'on s'était donné mais effectivement l'idée c'était d'abord de vulgariser.

Question 2-Je voudrais qu'on parle maintenant de l'auditoire cible de la série, à qui s'adresse la série, d'après mes recherches, on parle d'hommes âgés entre 25 et 54 ans

Le public de la série?… ah oui?

-Enfin celui de la chaine Explora d'après mes recherches

C'est plutôt les personnes âgées qui vont la

-Pour la série on parle d'un auditoire masculin, jeune, éduqué et nanti

Peut-être mais nous ce qu'on voulait vraiment honnêtement, le public cible au départ c'est sûre Explora elle a son public, et ça tu peux pas le réinventer, mais moi je l'ai fait pour que n'importe qui le comprenne. C'est à dire quand, au départ, je me disais

pas je m'adresse à des gens qui sont d'un milieu aisé et qui ont de quoi s'acheter un I Phone ou autre chose, je suis parti du principe que y'a beaucoup de gens qui sont connectés, même quand ils n'ont pas assez de moyen...tu sais les gens vont peut-être s'endetter pour s'acheter un téléphone, pour avoir du temps d'antenne, donc voilà pour moi c'était vraiment le grand public.

Question 3- Ta série traite de cybercriminalité comment tu l'abordes?

J'ai parlé à des experts qui auraient aimé que ce ça soit plus ci plus ça, je leur ai dit toi tout ce que tu connais déjà je peux pas te l'amener, c'est à dire c'est pas moi qui vais te faire connaitre ça, toi t'es l'expert qui va me permettre de transmettre cela à la population. Il me dit oué mais tu me comprend moi j'aurai fait ... après ce qu'il faut savoir c'est les moyens qu'on avait parque ça des fois les gens ils réalisent pas, tu sais combien de jours de tournages j'ai eu ?10 jours ! Entre interview, tournage, reconstitution, piège, *stunt*...et tout ça, 10 jours de tournage pas un de plus.

Question 4-J'aimerai qu'on revienne à la série et l'objectif derrière

C'était en tant que série au départ... c'était de vulgariser cet espèce de personnage que les médias décrivent des fois comme un criminel des fois comme un révolutionnaire des fois comme un espion, qui est le Hacker, ça fait quoi un hacker dans la vie? Et c'est quoi les différentes façons d'être un Hacker et c'est quoi les différents moments de la vie où citoyens on peut être confronté à ces phénomènes-là. Donc ça c'est le truc de départ, qu'est-ce que ça mange en hiver un hacker comme dirait l'expression québécoise. Après ça, il fallait décliner ça en 5 champs d'activités, et lui donner un style, lui donner un look, et ce qu'on s'est dit. Bon regarde là c'est la dimension informative c'est quoi un Hacker, on s'est dit bein si on fait de la télé si on fait du docu, faut qu'on donne une petite touche de plus. J'ai dit ok on va faire peur, on va essayer de faire peur, on va essayer de montrer qu'on s'en rend pas compte mais de nos jours, on est surveillés au quotidien sans s'en rendre compte, on le sait pas, on abuse de toute sorte de technique... D'ailleurs j'ai un autre projet sur lequel je travaille, plus léger....Donc l'objectif au départ je te disais, ok on va installer un climat de tension, de peur parce que tu le sais pas, tu le sais pas à quel moment tu vas être surveillé, tu sais t'arrives dans un café, tu te l*og* et hop et bien regarde un pamplemousse qui m'a détecté, c'est pas un vrai réseau, c'est quelqu'un qui essaye de voir si je vais pas régler un compte en banque, tu sais qui va peut-être voir s'il va pas avoir des informations personnelles sur moi, faire peur parce que...toi en tant que personnalité, si t'es une personnalité publique, tu peux facilement faire l'objet d'un ciblage, et d'une espèce de campagne de piratage, de la part de gens qui te voudraient du mal, pour une raison ou pour une autre. Toi entreprise privée bien en vue, et bien tu peux très facilement éveiller l'intérêt d'un concurrent ici ou ailleurs qui va vouloir

te saboter parce que ça va lui ramener ceci ou cela. Donc à chaque fois là on comprenait c'était de dire ou est la menace? Comment elle se pose ? De quelle façon elle s'installe et de quelle façon elle réussit à nous avoir? Donc c'était à peu près ça à chaque fois, c'était un peu une structure qu'on avait. Bien évidemment après tout dépendait de ce qu'on avait dans l'épisode par exemple l'épisode de Fred Savard bon là il accepte qu'on le pirate (Épisode 2), c'est pas le plus fort des épisodes honnêtement car je pense que techniquement y'a des problèmes. Je trouve qu'on avait pas le service, je trouve qu'on a pas été assez loin dans la prise de contrôle de ses données, mais parce qu'il y'avait une limite technique...tu vois. Et si je compare à l'épisode de Téo (Épisode 3). Ça c'est vrai, avec Fred on a fait de la mise en scène, avec Téo là, c'est une vraie prise de contrôle un vrai test d'intrusion qu'on avait avec eux et qui a fonctionné, tu vois...Mais l'esprit derrière, c'est toujours le même on va dire par quel moyen on va prendre le contrôle de ta vie numérique? Comment tu vas réagir à ça ? Et qu'est-ce que tu vas faire avant que tu t'en rendes compte? Qu'est-ce que nous on a le temps de faire avant que tu t'en rendes compte? C'est ça le truc, donc avec Fred c'était plutôt le truc rigolo. On s'amuse et on met des photos de Donald Trump sur son profil parce que c'est un mec qui se dit de gauche et tout ça...Mais avec Téo bein on les a appelé à partir du moment où on leur a dit c'est bon on a les mots de passe et les noms de certaines de vos dirigeants ça veut dire qu'on est rentré chez vous, ils nous ont dit: « ok bon d'accord, venez nous voir ».

Pour les Hacktivistes (épisode 5) donc pour les militants Hackers en ligne, c'était un peu différent. Ce qu'on voulait c'était faire un portrait de cette communauté. Je te dirais y'a deux visages aux hackers, y'a Robin des bois, qui est les Hacktivistes. Et y'a *Scarface* qui fait ça pour sa gueule, pour gagner du fric voilà. Et donc on voulait montrer que ces gens-là ils utilisaient les mêmes outils finalement, le truc...La complexité pour des forces de l'ordre et les gens qui les étudient, c'est qu'ils ont les mêmes outils, ils trainent dans le mêmes *chat room*, ils ont les mêmes espaces de dialogue ils sont tous sur *4chan*, ils sont tous sur *Reddit*, et puis sur les *IRC* à discuter. Mais tu sais pas quel est leur objectif, c'est à dire y'en a un son objectif c'est d'aller chercher de l'information du code, pour pouvoir s'attaquer à des corporations parce qu'il est anti corporation. Et l'autre bien lui, il veut du code tout simplement parce qu'il veut s'attaquer à des corporations parce qu'il veut chercher du fric chez les corporations. Il veut pas leur faire du mal...Il veut leur faire du mal peut être mais ce qu'il l'intéressé avant tout, c'est de gagner de l'argent. Et en plus, dans les organigrammes d'organisations criminelles, t'as toute sorte de gens qui sont employées et qui ont des bureaux. Tu sais, tu rentres ça l'air d'une *startup*, sauf que t'as lui qui est spécialisé dans le code pour percer les *firewalls*. Lui qui est spécialisé dans le hameçonnage. Lui qui fait ci, qui fait ça, puis ils sont payés par le crime organisé...Des fois ils le savent pas forcément, ils disent: « ok bein », tu sais c'est dans des pays ou la démocratie est un petit peu hésitante, y'a aucun problème, tu sais

tu vas te faire engager des fois par des criminels mais ça va profiter au gouvernement en fin de compte.

Donc l'idée c'était dans cet épisode la si je reviens aux Hacktivistes c'était d'essayer de montrer de quoi ça a l'air. Et ça a été très difficile parce que c'est pas facile à trouver. Y'a pas mal de gens que j'ai rencontré, j'ai pris des coups, des cafés avec des gens...Tout ça bein non, « tu filmes pas ma gueule, non ». Y'en a quelques-uns d'ailleurs ils m'avaient dit « oui », et un moment donné parce qu'on avait eu un problème dans la chaine de communication entre nous, ils m'ont dit...Ils m'ont envoyé un mail, ils étaient deux, ils m'ont envoyé un mail très précis, en me disant « Non je ne veux pas collaborer avec toi et je ne veux pas ni parler ni apparaitre dans ta série ». Après j'ai été les voir, ils m'ont dit « Parce que quelqu'un dans la chaine de communication entre nous qui s'est pas protégé, qui n'a pas crypté ses données ». Et là on sait pas, parce qu'ils sont harcelés par toute sorte de gens, parce que...Par des forces de l'ordre, par des boites qui veulent les engager. Parce qu'ils savent parce qu'ils se disent que ce sont des tranches... Ils sont surveillés, ils sont vraiment surveillés, c'est des gens extrêmement doués qui sont capables...Écoute, ils m'ont montré des trucs tu sais, t'en reviens pas, c'est fou. Ce qu'ils sont capables de faire et où ils sont capables de se rendre. Donc grosse recherche, on a fini par en trouver un qui a accepté et qui nous a fait son petit tour. Il nous a expliqué d'où il venait puis ça allait. Lui c'était vraiment le type Robin des bois, et cet épisode-là, c'était vraiment une espèce de portrait global des militants en ligne et de leur différentes factions. On avait...Bon, dans la série, on avait Gabriela Coleman de Concordia qui est vraiment une sommité en ce qui concerne Anonymous. Elle a écrit pleins de bouquins...Tu regardes sur Netflix, tous les documentaires sur Anonymous, elle est dedans, c'est une américaine, mais qui vit à Montréal. Donc l'idée c'était plus de faire le portrait de ça...Et dans ce qui est la sécurité des états (épisode 4), et bein comme y'a personne qui a voulu nous parler parce qu'ils se disent : « bein non mais on sait pas ». Tu sais, j'ai gratté, j'ai gratté, j'ai essayé. On m'a envoyé d'un bureau à autre, de la sécurité du ci du ça, mais ça fonctionnait pas. Personne voulait ouvrir sa gueule. Donc ce qu'on a fait, c'était du documentaire pur et simple classique. On a montré un peu l'historique de ça, les actions quelques actions célèbres, la centrale en Iran c'est un classique.

Question 5-C'est donc quoi le but de ce genre d'épisodes, le but de chaque épisode par rapport aux gens, est-ce que pour toi c'est juste le loisir ou est-ce que c'est plus poussé que ça?

Le loisir c'est le prétexte, c'est à dire on passe par le loisir, que les gens s'amusent en regardant la série, qu'ils aient du plaisir mais pour leur faire passer l'information qui est la suivante...À savoir que : trouver une clé USB par terre et la ramener chez soi, la brancher dans son ordi. Aller payer son compte alors qu'on est branché sur le wifi d'un café. Aller payer ses factures alors qu'on est branché sur le wifi d'un café, ou

encore, ne pas sécuriser son réseau à la maison. Et puis tu sais...Je sais pas moi, déshabiller ses enfants, donner le bain devant la télé intelligente, avec une caméra devant, tu sais pas où ça peut se rendre. C'est à dire que, l'idée ce qu'on voulait sortir de ça, c'est qu'on vit dans un univers connecté avec de plus en plus d'objets qui sont connectés, et un moment donné il faut se poser la question qu'est ce qui est enregistré par cette machine? Qu'est ce qui est transmis? Qu'est-ce que je fais avec ça ? Y'a des télés Samsung, dont on s'est rendu compte y'a pas longtemps qu'elles enregistraient le son, et qu'elles l'envoyaient à la centrale Samsung. C'est sorti y'a quelques mois, on fait quoi avec ça? Donc la question...Alors après y'a deux façons de réagir. La façon de réagir du milieu des Hackers c'est : « Je me protège vous n'auriez rien de ma vie, moi je suis un intégriste de la sécurité en ligne ». Voilà, et t'as pleins de gens qui disent « Bein pff de toute façon on a tout sur moi et j'ai rien à cacher ». Et le « j'ai rien à cacher » alors ils le prennent comme une insulte les Hackers. « Comment ça t'as rien à cacher, tu réfléchis pas, tu penses pas? T'as pas d'idée à toi ? T'as pas de vie intime ? » L'intimité on s'est rendu compte qu'elle a changé d'espace, et elle a changé de perception, tu prends un père, et une fille tu vois qu'ils n'ont pas la même notion de l'intimité. Un père et un fils, ils vont dire ça je m'en fou c pas ma vie intime, combien je gagne...mes fesses...ma gueule...pff rien à foutre. Alors que le père ou la mère vont dire « Attend ça va pas non ? Ça m'appartient tout ça ». Donc y'a un changement de paradigme, avec les générations ça c'est sure, mais l'idée c'est que l'intimité c'est aussi les choses que tu veux protéger pour qu'elles ne soient pas utilisées contre toi. Et y'a beaucoup de jeunes qui se rendent pas compte que des traces que tu laisses en ligne. Y'a des jobs maintenant de gens qui vont effacer ce que t'as été en ligne. Tu sais qui sont spécialistes de ça. Donc voilà pour cette épisode ce qu'on voulait c'était une prise de conscience, de se dire que les gestes anodins qu'on pose ont parfois une portée plus grande que ce qu'on pense, et qu'il faut se poser certaines questions

Question 6- Si on parlait maintenant de l'épisode 2 «le viol virtuel et l'intimidation», je me souviens c'est là où je pense que vous avez hacké le compte de la célébrité n'est-ce pas?

Exactement, ça c'était l'épisode que je te dirais le plus divertissement qui soit, parce qu'on prend une personnalité célèbre, et puis on lui propose...On lui lance un défi. Mais c'est quelque chose qui peut arriver à quidam...aussi évidemment, la prise de contrôle...Parce qu'aujourd'hui, là les gens, ils s'expriment sur les réseaux sociaux. Y a des personnages qui sont pas du tout des célébrités, des personnages publics, mais qui deviennent des célébrités sur les réseaux sociaux. À Montréal y'en a quelques-unes que je suis avec beaucoup d'intérêt. Et un jour y'a quelqu'un qui peut essayer de pirater ton compte Facebook, ton compte Instagram. Prendre le contrôle de ton email, et peut être rentré dans ta vie privée. Et donc y'a certains nombre de choses à faire. Euh...dans ce cas-là qui est très en lien avec le première épisode, mais je te

dirais que la raison n'est pas la même...La raison n'est pas la même car là, c'est la prise de contrôle de la vie de quelqu'un qui est plus exposé, et à qui on explique comment il devrait se protéger. Mais ça vaut aussi pour le commun des mortels, c'est à dire t'as beau ne pas être un personnage public, faire attention à tes mots de passe, sécuriser le wifi a la maison, t'assurer que tes machines ne sont pas complètement vulnérables, c'est un minimum.

Question 7-Mais on fait comment pour se protéger concrètement?

Y'a des VPN

-c'est quoi un VPN?

Virtuel personnel network c'est une application qui code tes données avant de partir et quand la personne les reçoit, elles sont décodées, mais y'a des VPN qui sont encore plus intéressant que çà et là c'est en lien avec l'épisode 3.

- *Le chapitre « Les États », ça tombe bien on est là, alors parle-moi de cette épisode*

Un VPN va a certain moment même déplacer ton adresse Ip, c'est à dire t'es sur internet, tu utilises un VPN et tu vas sur ses serveurs en Hollande, et bien tu vas te retrouver sur Netflix Hollande, tu vas te retrouver sur Google Hollande.

- C'est ce que font beaucoup de monde lorsqu'ils veulent se connecter sur Netflix Usa?

Exactement, ils utilisent un VPN, a une époque tu pouvais même faire ça avec Firefox, avec Mozilla Firefox parque c'est un VPN, WhatsApp un logiciel qui encode aussi même chose, c'est pas un VPN. C'est des données cryptés, tu peux pas les avoir comme ça. Par contre, une chose qui faut savoir, y'a un phénomène qui s'appelle les *five eyes*, Canada, États-Unis, Royaume Uni, Australie, Nouvelle Zélande. Ces cinq pays ont signés des accords de sécurité, et d'espionnage. Ce qui fait que leur agence de renseignements partagent toutes leurs données. Donc si tu utilises un VPN, et tu te dis « Je vais me mettre en Australie comme ça je vais être le plus loin possible », et bien il se trouve que les Australiens peuvent donner les données aux canadiens et aux américains. Si tu fais des choses qui sont reprochables qui sont pas irréprochables, et si tu choisis ton VPN même qui encode ici entre le Canada et aux États-Unis, c'est comme si tu fais rien parce qu'ils ont le droit d'aller saisir les données. Et un moment donné, ils vont pouvoir les utiliser, alors évidemment qui a peur d'utiliser internet,

c'est forcément des criminels. C'est que des fois dans le milieu des médias, tu fais des recherches, et tu rentres des mots clés dans ta recherche et ces mots clés tout a coup ça fait une petite étincelle quelque part sur les réseaux ça fait *tttzzzz* dans les agences de sécurité. Et du coup « Ah tien il a écrit AL QAIDA », si t'es journaliste, ils vont dire « Ah ok c'est un journaliste, mais on va surveiller quand même ». Donc le truc c'est que dans la guerre des pays, on voulait montrer que y'avait une guerre mondiale qui a lieu tous les jours, mais qu'on se rend pas compte. Parce qu'elle est extrêmement cachée, elle est souterraine, elle se passe sur les réseaux, sur internet. Mais les gens se font des vacheries, en général, ils ne signent pas leurs...ils les signent, mais jamais ils le reconnaissent, STUXNET c'était énorme.

- *Bein oui, c'est comme aussi l'affaire Sony*

Voilà, Sony. Sony, on s'est dit voilà est ce que c'est les Nord-Coréen, est ce que c'est les Chinois qui ont aidé les Nord-Coréens.

Question 8- Dans cette épisode, tu parles de cyberguerre, les gens tu penses qu'ils comprennent ce que c'est une cyberguerre, parque y'a pas d'arme, pas de violence et pour eux la guerre c'est Boom, donc est ce que les gens ont conscience de c'est quoi une cyberguerre, et qu'une guerre t'as pas forcément de la violence ou des armes?

T'as vu la carte des attaques de *North...North* c'est une compagnie qui répertorie les attaques. T'as l'impression que c'est la guerre mondiale, ça vient de Chine, ça vient de...Bon évidemment, la cible c'est les États-Unis, parce que y'a beaucoup entreprises américaines qui sont des multinationales, qui ont leur serveurs en Californie, et qui sont attaquées par tout le monde quoi. Mais oui effectivement l'idée la dedans, c'était qu'on se rende compte que finalement, nos états sont en conflit pas ouverts, car ils veulent pas que ce soit ouvert parce qu'ils font des choses qui ne sont pas forcément légales. On dit toujours que les Chinois espionnent, mais tout le monde espionne et tout le monde espionne.

-Bein oui y'a eu l'affaire qui avait fait scandale entre l'Allemagne et les États unis

Oui la NSA, ça c'était les écoutes, exactement.

Question 9-Pour toi comment on se protège d'une cyberattaque, est ce que c'est vraiment l'utilisation des VPN, est ce que ça touche les gens ce genre d'attaques comme on voit dans l'épisode et le chapitre 3 est ce que ça touche les gens?

Tu veux dire la cyberguerre?

- *Oui pardon la cyberguerre?*

Tu ne peux pas te protéger contre ça parce que ce sont des gens beaucoup plus qualifiés que toi en général. Tu sais, moi je ne peux pas me protéger d'un hacker chinois, je peux me protéger en achetant un mac, car statistiquement y'a beaucoup moins de virus.

- *Mais faut quand même couvrir ta cam?*

Ça c'est le truc de base, même si moi je le fais pas, mais tu vois, tu couvres ta caméra, t'as des mots de passes un peu compliqué que tu changes régulièrement, t'essayes quand tu fais des recherche un peu sensibles...Bein t'essayes de les faire avec *Reunion rider* Tor qui est le logiciel de furetage, qui lui aussi est une forme de VPN...Lui c'est un VPN...Mais maintenant quand tu télécharges TOR.

- Mais on peut plus télécharger TOR non?

Voilà le problème c'est que maintenant quand tu télécharges TOR tu es surveillé, donc ce que ça te prend ça prend un VPN qui délocalise ton adresse IP pour pouvoir télécharger TOR, et l'utiliser.

- *Mais tu télécharges dans aucun des 5 pays enfin avec aucune adresse IP des 5 pays?*

Voilà exactement c'est ça

-Ça commence à devenir complexe tout ça pour le commun des mortels

Mais quand tu rencontres un Hacker, il a une quincaillerie avec lui...Ils ont un sac à dos, puis là ils ont ...ça c'est une prise pour pouvoir changer les codes de wifi, ça c'est comme un pamplemousse, pour pouvoir agrandir mon réseau mais c'est différent...Ça c'est pour aller chercher...Bein pour voir ce que les gens font pour voir si je suis pas surveillée...Ils se baladent avec un sac à dos, c'est un cube comme ça et puis voilà.

Question 10- J'aimerai qu'on parle maintenant de l'épisode 4 «les entreprises»:

Bein là ce qu'on voulait c'était montrer qu'une entreprise qui est techno soucieuse de ce qui se passe autour d'elle. Tu sais c'est Téo, donc ça marche par application. C'est

des gens qui sont reliés à Taillefer, qui fait du jeux, même eux finalement peuvent se faire avoir si tu trouves le bon angle. Le bon angle c'est l'ingénierie social, *social engineering*. Faut que tu sois un peu vicieux, et que tu fasse croire des choses aux gens, donc qu'est-ce qu'on fait croire aux gens? Le mec il crée une adresse internet qui ressemble beaucoup à celle d'Alexandre Taillefer. Bon on dit juste un dirigent mais dans ce cas-là c'était Alexandre Taillefer...Et qui dit : « Mais qu'est-ce que c'est cette pub de *Uber*? Ils me matent la laine sur le dos, faut qu'on fasse quelque chose. » Les gens ils revoient, ils voient le boss ! Le boss, il m'a envoyé un truc et il est pas content, et évidemment, t'as ouvert le truc, t'as été voir la pub, et hop voilà tu es hameçonnée tu m'appartient, et je fais ce que je veux avec toi, et ça se déplace partout...Le problème, ce qu'on voulait montrer, c'est que nos données, en tant qu'individus, en tant qu'usagers, que personnes privées, se retrouvent sur des serveurs qui appartiennent à des compagnies avec qui ont fait affaire. Comme des banques, comme des compagnies de services et que si elles sont pas sécurisées, et bien ça peut nous montre en danger éventuellement nous. Eux se mettent en danger, mettent en danger la vie privée de leur employées, parce que finalement si t'as les mots de passe et les noms d'usager, tu peux savoir où il vit, tu peux savoir s'il a une double vie, s'il a des enfants, si ses enfants ont des problèmes ou des maladies, s'ils était vraiment en voyage au Mexique, ou s'il était à Paris avec quelqu'un d'autre. Tu sais, tu vois tout ça la tout ça finalement c'est en danger et toi usager ils ont ta carte de crédit, bon ils ont des façons de crypter, la dessus ils avaient un bon outil de cryptage de données de carte de crédit, mais y'a beaucoup beaucoup d'éléments là-dedans qui fait qu'on se retrouve avec nos données dans toute sorte de corporations qui sont pas forcément toujours bien protégées. Le pire étant les banques évidemment la tu sais, parce que Téo mine de rien, ils faisaient gaffe, et ils se sont fait avoir par quelqu'un qui a pas lâché, qui s'est dit je vais vous avoir. Mais y'en a d'autres qui font pas autant attention, et on se fait avoir régulièrement...Donc l'idée c'était de dire que dans les entreprises, il faut qu'on soit protégés, il faut que les entreprises se protègent et nous protègent aussi et c'est à eux que ça incombe je te dirais, parce que nous, c'est pas rentable de pirater un individu. T'imagine ? Ok je vais faire toute la rue Berri, et je vais essayer d'hameçonner monsieur du 6581, monsieur du 6583, 6585...Non alors que tu t'attaques a une belle grosse compagnie, pis la, tas des tas de fichiers de clients, et d'usagers et tu peux piger la dedans, voilà c'est un peu ça l'idée.

-Mais justement n'as-tu pas eu peur de faire peur aux gens... Je veux dire tu fais peur aux gens y'a l'intrigue mais les gens ils vont juste paniquer non?

Non, mais tu vois que Téo, il ont dit on va prendre les mesures qu'ils faut, Téo bien regarde Téo, en fait c'est un très bon exemple, ils ont pas paniqué, ils ont dit bein merci on va prendre acte de cela, c'est à dire que eux ce qu'ils veulent, c'est pas pour rien qu'ils ont accepté, ils voulaient savoir jusqu'où ils peuvent se rendre.

-Ils ont fait de l'audit quoi

Exactement

-Ils ont pris un consultant en cyber sécurité quoi,

Oui un *testing* gratuit, ils ont pris ça comme ça et de ce point de vu là c'est très intelligent et puis attend dans les États

Les États, il y'a tout ce qui est nos données dans notre état, les impôts les systèmes de santé, les systèmes éducatifs, tout ça c'est des millions et des millions de pages qui sont stockées un peu partout dans des serveurs qui sont pas forcément bien sécurisés. Et la sécurité des états elle passe aussi par ça, elle passe par nos données…Tu sais le bulletin de santé de notre Premier ministre, de notre ministre de la défense.

-Donc tu arrives à tomber sur le dossier santé de notre Premier ministre, tu sais qu'il a une allergie aux arachides, personne ne le sait sauf les gens du protocole, et tu t'arranges pour faire en sorte de faire rentrer quelqu'un au moment où on sert le repas dans un G7 ou un truc quelque part, et tu fais en sorte qu'on lui serve des arachides....Et hop, ni vu ni connu, ça peut paraitre fou que ça mais c'est quelque chose qui pourrait arriver?

Tout à fait, c'est à dire que y'a pas que la guerre mais y'a la sécurité intérieure, la sécurité intérieure ça joue beaucoup et ça dépend beaucoup de la façon qu'on a de protéger les données dans nos agences gouvernementales. Y'a des gens qui ont perdu des disques durs, y'a des gens qui ont perdu des ordinateurs, ça ça arrive dans les compagnies privées…Y'a un mec qui a perdu un lap top en Chine, il bossait pour Prat and Whitney.

-Bravo, il a choisi l'endroit

Prat and Whitney, c'est le rêve en plus, c'est les réacteurs, les moteurs d'avion tout ce que tu veux

- Et en chine en plus, l'idéal quoi

Voilà, non ça c'est un gros souci, et il faut qu'ils en entendent parler, parce que maintenant y'a des attaques contre des hôpitaux qui sont spécifiquement ciblés, et les hôpitaux devraient en fait prendre acte de cela, et même faire des tests et inviter des

gens comme nous. Tu sais on n'a pas pu filmer dans un hôpital on n'a pas pu...Je m'étais rendu, j'ai appelé a peu près tous les grands centre hospitaliers autour de Montréal pas juste à Montréal, et y a deux personnes qui ont répondu, mais y'en a une finalement...les gens des com lui ont dit non non ça ça passe par nous d'abord.

-En même temps, je comprends, parque si jamais vous mettez en lumière que y'a une faille dans leur système...

Ah bein, ils vont recevoir un appel de Barrette c'est clair, lui c'est du style si jamais y'a un problème c'est moi qui t'appelle, donc voilà l'idée, c'est si y'a une faille faut l'exploiter et faut la corriger.

Question 11- Est ce que le but de la série c'était que les gens changent leur habitudes à différents niveaux?

Oui, l'idée c'était de vulgariser ça et que les gens partent avec une information de ça et après c'est à eux de décider, est ce qu'ils veulent protéger leur vie privée et prendre des précautions ou considérer que de toute façon tout se sait déjà à leur sujet et je m'en manque. Ça fait partie de la nouvelle vie qui est le parti pris de pas mal de gens, en disant : voilà regarde tout est ouvert, tu peux chercher tout ce que tu veux...Moi je le sais maintenant quand je vais aux États-Unis ils savent tout sur moi. Ça dure deux secondes à la frontière...ça dure deux secondes...Ils savent que je fais des films ils savent que je fais ci, ils savent que je fais ça.

Question 12-Est ce qu'il y'a un côté éducatif dans la série?

Le coté éducatif, très certainement, on voulait sensibiliser les gens à cette réalité-là et les laisser avec l'information et puis peut-être c'est à eux ensuite de creuser ensuite, et de fouiller, Mais leur ramener des données comme *VPN, cryptage, hameçonnage, vie numérique, vie virtuelle*...Tout ça, ça te fait dire: Ok finalement ça se fait pas tout seul seulement, toi tu rentres ton nom, ta carte de crédit et ton mot de passe, et hop super tu peux utiliser Google Amazone, Apple, Ticket master, tout ça t'as un profil la... Et il faut que tu réfléchisses où ça va?

Question 13-C'est intéressant donc finalement comment la série communique, elle communique justement à travers le format car c'est un format qui va attirer les gens?

Exactement l'idée c'était de trouver les bonnes métaphores visuelles pour amener les gens à comprendre ce qu'on avait à leur dire, donc y'a l'espèce de tuyauterie, parque c'est ça... C'est de la tuyauterie avec des systèmes et des réseaux qui passent et de

temps en temps t'as un espace de vapeur et un petit individu qui se promène dedans alors qu'il est pas censé être là. Tu as l'intérieur de l'ordinateur qui est l'espèce de mécanique à travers laquelle s'immiscent les pirates, et puis les espèces de *glitch* numériques...En se disant, tiens eux ce qu'ils font c'est qu'ils rentrent dans un protocole, ils causent des petits cours circuits pour pouvoir s'immiscer, ils se créent des petites portes d'entrée dans ton système...Qu'est-ce que j'avais d'autre... Ah oui, j'avais aussi le clavier transparent, ça c'est pour dire, regarde tu crois que ton clavier il est dur, y'a des gens qui t'espionnent d'en dessous. Et toi quand tu poses ton doigt ici, ça crée une empreinte, une emprunte qui est enregistrée, qui est envoyée et qui est décortiquée et évidemment parfois répliquée pour pouvoir prendre ta place

-Ça c'est le côté métaphorique visuel qui vient finalement consolider le message que l'auditoire en général va comprendre donc visuellement ça va plus conforter cette information?

Exactement, l'idée c'était de montrer des réseaux, la tuyauterie, des serveurs, des intérieurs d'ordinateur, de dire qu'on rentre dans la machine, on rentre dans la machine et qu'on la fait sans rayer, et de se dire qu'un moment donné y'a quelque chose qui fonctionne pas... Tu sais c'est comme bug, bug c'était vraiment des insectes qui rentraient dans les grands ordinateurs et qui bouffaient une carte. Tu sais c'était des cartes perforées, donc c'était de la lecture de cartes perforées, c'était vraiment du code binaire, là le langage à l'époque. Donc si jamais tu bouffais un bout du carton, bien c'est finit ton code était plus valide.

Question 14-Parmi les profils d'usagers, on a tendance à penser que ce sont les jeunes qui sont les plus vulnérables c'est bien le cas?

Les ainés aussi

-Ah bon pourquoi ?

Bein oui les ainés parce que les ainées :

- oui bonjour madame Tremblay, c'est Steve, Steve vous savez l'ami de votre petit neveu Nicolas

- ah Nicolas bien oui oui

- Hey Nicolas va pas bien

- Comment ça qu'est-ce qu'il a faite Nicolas,

Tu sais c'est le truc classique, tu sais, vous devez réinitialiser votre compte, vous devez changer votre mot de passe, prière de suivre ce lien, appelez nous, nous devons faire une vérification sur votre carte de crédit, quelqu'un a tenté de pirater votre compte on veut vérifier des informations de sécurité, tu sais tu passes par la peur, tu leur fait peur et ils rentrent dans le truc et ils se font avoir, c'est énorme ce qu'il se fait tout le temps.

Par rapport aux jeunes, c'est plutôt au niveau de la sécurité de la vie privée. Ça va être l'imprudence, ne pas se projeter en avant, ne pas se dire qu'un employeur dans 10 ans, il va peut-être regarder ton profil puis il va voir que t'étais à 4 pattes bourré sur la table de la mariée et que t'as gâché le mariage des gens. Et puis il va remonter le fil... ah ok ah c'est ça que les gens disaient, c'est comme ça qu'il a réagi, tu vas prendre des positions politiques.

Tu sais pas un moment donné, ça bouge tellement ça change tellement, je vois les gens ils suivent des profils, Snapshat, et c'est fini Snapshat, Instagram, et c'est finis Instagram.

Faut faire attention à l'utilisation des réseaux sociaux, moi je les utilise pour promouvoir mes films. C'est pas moi le produit, c'est apprendre à utiliser ce qu'ils nous offrent pour trouver notre intérêt en sachant que si y'a notre intérêt et que si c'est gratuit c'est que c'est toi le produit.

Pourquoi? Bein parce que t'as un certain nombre de méta données qui vont circuler et t'es pas un individu, t'es même plus un individu, tu es une petite machine dans un... Tu fais partie d'un prix de gros, toi l'individu, ils s'en foutent. Ce qui les intéresse c'est la grosse liste qu'ils vont s'échanger très cher. On est même plus des individus, on est des fourmis, on est des membres d'un...Comment dire d'une grosse toile que les gens vont vendre et pour lesquelles ils vont faire du cash.

APPENDICE A

CERTIFICAT D'ÉTHIQUE

Groupe en éthique
de la recherche
Piloter l'ethique de la recherché humaine

EPTC 2: FER

Certificat d'accomplissement

Ce document certifie que

sara nacer

a complété le cours : l'Énoncé de politique des trois Conseils :
Éthique de la recherche avec des êtres humains :
Formation en éthique de la recherche (EPTC 2 : FER)

16 mai, 2017

BIBLIOGRAPHIE

Anadón, M. Guillemette, F. (2006). La recherche qualitative est-elle nécessairement inductive? Recherches qualitatives 5 (2006): 26-37. Récupéré de http://www.recherche-qualitative.qc.ca/Revue.html

Bardin, L. (1977). *L'analyse de contenu.* France : PUF

Barreau-Brouste, S. (2013). Le documentaire télévisé : les enjeux d'une définition controversée. *Institut national de l'audiovisuel.* Récupéré de https://www.ina-expert.com/e-dossier-le-documentaire-un-genre-multiforme/le-documentaire-televise-les-enjeux-d-une-definition-controversee.html#5

Benayoun, G. (1990). Les hauts et les bas du documentaire français. *Le Film français n°2294, 9 février 1990, p. 16.* Récupéré de https://www.ina-expert.com

Benghozi, P-J. Bureau, S et Massit-Folléa, F. (2012). L'internet des objets : quels enjeux pour l'Europe. Paris : Éditions de la Maison des sciences de l'homme. Récupéré de http://books.openedition.org/

Blog lefigaroux (2009). *Les chaînes spécialisées laissent-elles encore une raison d'exister aux chaînes généralistes* ? Récupéré de https://lefigaroux.wordpress.com

Boutet, A. Trémenbert, J (2009) Mieux comprendre les situations de non-usages des TIC. Le cas d'internet et de l'informatique. Réflexions méthodologiques sur les indicateurs de l'exclusion dite numérique ». *Les Cahiers du numérique, 2009/1 (Vol. 5), p. 69-100.* Récupéré de https://www.cairn.info/revue-les-cahiers-du-numerique-2009-1-page-69.htm

Bryson, Lyman (1948). *The Communication of Ideas.* New York: The Institute for Religious and Social Studies.

Castells, M. (2001) La Galaxie Internet. Paris : Fayard.

CCNPPS (2010) Comprendre les communications médiatiques. L'approche encodage/décodage. Récupéré de http://www.ccnpps.ca/docs/2010_ProcessusPP_SI2010_ComprendreComMedia_Fr.pdf

Centre d'études sur les Médias (2017) *La télévision.* Récupéré de http://www.cem.ulaval.ca/pdf/Television.pdf

Centre national de ressources textuelles et lexicales. (2012). Communication. *Outils et références pour un traitement optimisé de la langue.* Récupéré de http://www.cnrtl.fr/definition/communiquer

Daily Sabah Health (2017). Internet addiction poses grave danger for teens, study reveals. Récupéré de https://www.dailysabah.com/health/2017/08/10/internet-addiction-poses-grave-danger-for-teens-study-reveals

Dasgupta, D. and M. Ferebee, D. (2013). Consequences of diminishing trust in cyberspace. *The Proceedings of the 8th International Conference on Information Warfare and Security: ICIW 2013. Academic Conferences Limited, 2013.* Récupéré de https://books.google.ca

Desarnaud, G. (2017). *Faire face au risque.* France : Ifri. Récupéré de https://www.ifri.org/

Dépelteau, F. (1998). *La démarche d'une recherche en sciences humaines: De la question de départ à la communication des résultats.* Québec: Les Presses de l'Université Laval.

George, É., & Granjon, F. (2008). *Critiques de la société de l'information.* Paris: Harmattan.

Georges, F. (2009). Représentation de soi et identité numérique. Une approche sémiotique et quantitative de l'emprise culturelle du web 2.0 ». *Réseaux, 2009/2 (n° 154), p. 165-193. DOI : 10.3917/res.154.0165.* Récupéré de https://www.cairn.info/revue-reseaux-2009-2-page-165.htm

Ghernaouti-Hélie, S. (2009), La cybercriminalité: le visible et l'invisible. Lausanne : Presses polytechniques et universitaires romandes

Granjon, F. et Denouël, J. (2010). Exposition de soi et reconnaissance de singularités subjectives sur les sites de réseaux sociaux. *Sociologie, 2010/1 (Vol. 1), p. 25-43. DOI : 10.3917/socio.001.0025.* Récupéré de https://www.cairn.info/revue-sociologie-2010-1-page-25.htm

Grenier aux nouvelles (2015) ICI Explora: un succès d'abonnement et d'écoute. Récupéré de http://www.grenier.qc.ca/nouvelles/8598/ici-explora-un-succes-dabonnement-et-decoute

Hackerwifi.net (s. d.). Hackers Récupéré de http://www.hackerwifi.net/

Hall, S. CCCS, Albaret Michèle, Gamberini Marie-Christine. (1994) Codage/décodage. [Chapitre de livre] In: Réseaux, volume 12, n°68, 1994. Les théories de la réception. (p.27-39); Récupéré de www.persee.fr/doc/reso_0751-7971_1994_num_12_68_2618

Hall, S. (2007). *Identités et cultures: Politiques des Cultural Studies*. Paris: Amsterdam.

Harvey, P-L. (1995). *Cyberespace et communautique.* Québec: Presses de l'Université Laval. Récupéré de https://books.google.ca

ICI Explora (2016). *HACKERS.* Récupéré de http://ici.exploratv.ca/emissions/hackers

Jordan, T. and P. Taylor (2004) *Hacktivism and Cyberwars: Rebels With a Cause?* London: Routledge. Récupéré de https://books.google.ca

KAP Tactiques numériques. (2017). *les chiffres du numérique au Canada en 2017.* Récupéré de http://www.kap-numerique.com/chiffres-numerique-canada-2017/

Lasswell, H. (1927). Propaganda Techniques in the World War I, New York : Knopf récupéré de http://www.mei-info.com

Lech J. Janczewski, Andrew M. Colarik, (2008) Cyber Warfare and Cyber Terrorism. New York : Information Science Référence. Récupéré de http://books.google.com/

Lienmultimedia. (2013). Explora lance une campagne ciblant les amateurs de sports. Récupéré de http://www.lienmultimedia.com/spip.php?article36211

Mahan, Robert E., et al. (2011). Secure data transfer guidance for industrial control and SCADA systems. *No. PNNL-20776. Pacific Northwest National Laboratory (PNNL), Richland, WA (US), 2011.* Récupéré de http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-20776.pdf

Mattelart, A. Neveu, É. (1996) Cultural studies stories : La domestication d'une pensée sauvage? Réseaux, n° 20. p.29. Récupéré de http://www.enssib.fr/autres-sites/reseaux-cnet/80/01-matte.pdf

McGoogan, C. (2017, 8 mars). Why your smart TV is the perfect way to spy on you. *The Telegraph.* Récupéré de http://www.telegraph.co.uk/technology/2017/03/08/smart-tv-perfect-way-spy/

Mehl, D. (1992). *La Fenêtre et le Miroir. La télévision et ses programme.s.* Paris : Payot, collection « Documents ». p. 156. Récupéré de https://www.ina-expert.com

Millerand, F. (2008) David Morley et la problématique de la réception. *Commposite 1.1 (2008): 61-70.* Récupéré de http://www.commposite.org/index.php/revue/article/view/8/7

Morley, D. (1992). *Television, Audiences and Cultural Studies.* Londres : Routledge

Morley, D. Dayan, D. (1993) La réception des travaux sur la réception. Retour sur « Le Public de Nationwide ». *Hermès, La Revue 1993/1 (n° 11-12), p. 31-46.* Récupéré de https://www.cairn.info/load_pdf.php?ID_ARTICLE=HERM_011_0031

Petersen, H. Baccelli, E. Wahlisch, M. (2014). Interoperable Services on Constrained Devices in the Internet of Things. Récupéré de https://www.w3.org/2014/02/wot/papers/baccelli.pdf

Publicaffairsbooks (s. d.). Récupéré de http://www.publicaffairsbooks.com/book/the-hacked-world-order/

Québec. Cabinet de la Ministre de l'Économie, de la Science et de l'Innovation (2017) *Stratégie québécoise de la Recherche de de l'Innovation 2017-2022* [Communiqué]. Récupéré de https://www.economie.gouv.qc.ca/fileadmin/contenu/documents_soutien/strategies/recherche_innovation/SQRI/sqri_complet_fr.pdf

Radio-Canada (2016) *La série HACKERS lève le voile sur le monde obscur des pirates informatiques.* Récupéré de http://servicesfrancais.radio-canada.ca

Radio-Canada. (2017, 21 novembre). Piratage massif chez Uber : les données de 57 millions de personnes dérobées. Radio-Canada.ca. Récupéré de http://ici.radio-canada.ca/nouvelle/1068600/transport-uber-faits-divers-piratage-donnees-personnelles

Radio-Canada. (2017, 20 novembre). 290 millions pour offrir Internet haute vitesse à 100 000 foyers en région. Radio-Canada.ca Récupéré de http://ici.radio-canada.ca/nouvelle/1068198/quebec-ottawa-internet-haute-vitesse-region-investissement.

Radio-Canada International (2016). Internet à domicile : le Québec de plus en plus connecté. Récupéré de http://www.rcinet.ca/fr/2016/11/03/internet-a-domicile-le-quebec-de-plus-en-plus-connecte/

Raymond, É. (2000). Comment devenir un hacker [Chapitre de livre] Dans *Olivier Blondeau, Libres enfants du savoir numérique (p. 255-277)* Paris: Editions de l'Éclat « Hors collection ».

Rocare (s. d.) *Extrait de guides pour la Recherche Qualitative*. Récupéré de http://www.ernwaca.org/panaf/RQ/fr/definition.php

Segal, A. (2016, 22 février). New Cyber Brief: Protecting Data Privacy with User-Friendly Software [Billet de blogue]. Récupéré de https://www.cfr.org/blog/new-cyber-brief-protecting-data-privacy-user-friendly-software

Segal, A. (2016) The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age. New York : Public Affair Tm. Récupéré de http://books.google.com/

Ségur, C. (2015). L'étude des publics de télévision en SIC. Quelle évolution conceptuelle ? , Revue française des sciences de l'information et de la communication [Online], 7 | 2015. DOI : 10.4000/rfsic.1470 Récupéré de : http://rfsic.revues.org/1470

Wanlin, P. (2007) L'analyse de contenu comme méthode d'analyse qualitative d'entretiens: une comparaison entre les traitements manuels et l'utilisation de logiciels. Recherches qualitatives 3 (2007): 243-272. Récupéré de http://www.recherche-qualitative.qc.ca/documents/files/revue/hors_serie/hors_serie_v3/Wanlin2.pdf

Wolton, D. (2005) Il faut sauver la communication. *Revista FAMECOS Porto Alegre nº 27 agosto 2005 quadrimestral.* Récupéré de http://revistaseletronicas.pucrs.br