UNIVERSITÉ DE LORRAINE | UFR SCIENCES HUMAINES ET SOCIALES - METZ

crem centre de recherche EA 3476 sur les médiations communication, langue, art, culture

Master 1 --, Mention Information communication
Spécialité Création de projets numériques

Du hacker au cybercriminel :

Imaginaires socio-culturels et représentations professionnelles

Présenté par

Quentin Mores

Directrice de recherche : Marie Chagnoux

Année universitaire 2019-2020

Remerciements

Je remercie Mme Marie Chagnoux et l'ensemble des personnes qui m'ont aidé à réaliser ce travail de recherche (M. Franck Bettanier, M. Nicolas Chevrier, Mme Anne Souvira, …). À toutes les personnes qui ont cru en moi tout au long de mon parcours scolaire et universitaire.

Table des matières

Introduction

Le 31 août 2017, "OxyMonster" de son vrai nom Gal Vallerius, un français âgé de 38 ans, est arrêté par la police américaine pour trafic international de stupéfiants depuis le *Dark Web*[1]. Il sera condamné un an plus tard à vingt années de réclusion criminelle aux États-Unis.[2] Bien loin des stéréotypes des œuvres culturelles contemporaines, ce cybercriminel d'envergure bouscule les codes et nous amène à nous poser plusieurs questions au sujet de la représentation du cybercriminel aujourd'hui. Ce n'est pas un jeune surdoué de l'informatique, portant des gants et un sweat à capuche, à l'hygiène de vie passable qui vit au domicile familial dans une ambiance sombre. Gal Valerius habite dans un village en campagne bretonne, âgé de 39 ans, il vit avec sa femme et éprouve une certaine passion pour les barbes et moustaches. Ce travail de recherche a pour objectif de comprendre comment s'est construite la représentation d'une figure numérique encore peu médiatisée il y a une dizaine d'années, celle du cybercriminel. La lutte contre la cybercriminalité et par conséquent le développement de la cybersécurité sont devenus un enjeu de taille pour toutes les institutions qu'elles soient étatiques ou commerciales. Nous pouvons mentionner pour la France, la création de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) en 2009. L'intérêt est de tendre à mieux appréhender ce qui influe dans la construction de cette représentation et quels sont les acteurs et processus qui interviennent dans cette construction. Dans une posture sociologique, nous étudierons un corpus de différentes œuvres culturelles ainsi que des entretiens avec des professionnels du numérique et de la cybercriminalité afin d'apporter des éléments de réponses à notre problématique : quelle est la représentation du cybercriminel aujourd'hui ? Comment s'est construite cette représentation ? Quelle en est la portée sur le terrain professionnel ?

Nous verrons que cette représentation est le résultat d'un long cheminement qui trouve ses sources dans différents faits historiques, dans plusieurs courants de pensées, dans des appropriations et des usages étymologiques variés de la part de multiples acteurs (médias, organisations, …). La cybercriminalité et la figure numérique du cybercriminel ne sont encore que peu explorées dans les Sciences Humaines et Sociales, s'interroger sur cet objet d'étude permet d'aborder d'autres figures des Technologies de l'Information et de la Communication en insistant sur la puissance des imaginaires de l'informatique.

[1] *cf.* Glossaire
[2] http://www.leparisien.fr/faits-divers/etats-unis-20-ans-de-prison-pour-le-franco-israelien-oxymonster-trafiquant-du-dark-web-10-10-2018-7915167.php

1. Du *hacker* aux cybercriminels : une histoire complexe

Pour comprendre comment la représentation du cybercriminel s'est construite dans les imaginaires, il est nécessaire de convoquer les auteurs de plusieurs champs complémentaires : celui de l'histoire d'Internet, pour éclairer les origines, celui de la technique pour éclairer la diversité des pratiques et celui de la langue pour expliquer les termes.

1.1. Les origines

Tout d'abord, il est important de comprendre les origines d'Internet car elles ont accompagné et nourrie la cybercriminalité et sa représentation telles que nous les connaissons aujourd'hui. Il est nécessaire de passer par cette histoire pour mieux cerner notre objet d'étude qui y trouve ses racines.

1.1.1. La genèse

La genèse d'Internet débute dans les années 1960 avec des projets militaires américains de recherches scientifiques dont le plus abouti : ARPANET (pour *Advanced Research Projects Agency Network),* qui est officiellement dévoilé en octobre 1972. ARPANET est le premier réseau informatique qui est développé à grande échelle aux États-Unis, le réseau voit d'ailleurs l'apparition du protocole de transfert de données que nous utilisons encore aujourd'hui, le protocole TCP/IP (*Transmission Control Protocol/Internet Protocol).* L'objectif du réseau est de pouvoir faire face militairement à l'éventualité d'une attaque nucléaire de la part de l'Union soviétique ; il faut que l'armée américaine décentralise l'information afin qu'elle ne soit plus accessible par l'intermédiaire d'un seul et unique serveur. Dès son origine, ARPANET est le résultat d'une collaboration militaire et scientifique car conjointement aux recherches militaires de personnes telles que Robert Elliot Kahn de la DARPA (*Defense Advanced Research Projects Agency*), l'agence gouvernementale en charge d'ARPANET, ce sont également des universitaires, scientifiques, ingénieurs comme Douglas Carl Engelbart du SRI *(Stanford Research Institute*) ou encore Vinton Gray Cerf de l'UCLA (*University of California, Los Angeles*) qui contribuent à son élaboration. L'idée de mettre des ordinateurs en réseau pour transmettre des informations suit naturellement le développement de l'ordinateur et de l'informatique. On constate déjà, depuis cette période, une forte implantation californienne du réseau des réseaux qui n'est pas sans rappeler la localisation géographique des GAFAM (Google, Apple, Facebook, Amazon et Microsoft) que nous connaissons aujourd'hui et qui constituent les principaux acteurs d'Internet à l'heure actuelle.

À partir des années 1980, ARPANET fait son entrée dans les universités américaines ce qui amène progressivement à un changement de terminologie au profit d'Internet. De nouveaux principes ainsi qu'une nouvelle idéologie naissent de ce nouveau réseau qui se sépare de son engagement militaire des décennies passées.

L'arrivée des premiers ordinateurs, encore très couteux, dans de grandes universités américaines obligent les étudiants à suivre de multiples règles pour pouvoir accéder à l'outil ; ce qui va, en outre, pousser à l'élaboration du premier ordinateur portable quelques années plus tard notamment. Les étudiants s'organisent alors pour accéder aux machines informatiques en dehors des heures prévues à cet effet pour profiter au maximum du potentiel offert par cette nouvelle technologie.

Une période d'euphorie suit le développement d'Internet dans le champ universitaire en lien direct avec la contre-culture américaine de l'époque ce qui encourage son amélioration. Patrice Flichy, au travers des propos d'Howard Rheingold, journaliste et essayiste influant sur le sujet durant cette période, souligne l'importance que prennent les communautés virtuelles : « il insiste notamment sur le fait que les communautés virtuelles ne sont pas des utopies, puisqu'elles ont été réalisées. […] Il en fait le modèle de référence d'Internet, alors que le changement d'espace social de référence modifie fondamentalement la situation : le mode de fonctionnement des communautés contre-culturelles ou de l'université n'est évidemment pas celui de toute la société » (Flichy, 2001 : 114). Dominique Cardon évoque quant à lui le cas de la communauté virtuelle *The Well* qui constitue « la plus célèbre des communautés virtuelles » qu'il définit comme « un espace de discussion électronique organisé en forums thématiques » (Cardon, 2010 : 24).

Les communautés virtuelles se trouvent au centre des attentions dans les médias. Internet, bénéficiant d'une image plus que positive, se voit progressivement ouvert à la société : entreprises, organisations, politiques, tout le monde souhaite profiter de ce nouvelle espace unique pour la démocratie et le commerce. De plus, la mise en réseau de l'hypertexte en 1990 avec le langage HTML (*Hypertext Markup Language*) va centraliser l'ensemble de l'information au travers des navigateurs, apportant cet aspect de maillage. Dominique Cardon parle d'un passage au Web à ce moment avec le fait que « le navigateur donnera alors à l'utilisateur l'impression de faire face à un objet homogène, mondial et infini » (Cardon, 2010).

Seulement, après cette période prolifique (contenus proposés toujours plus nombreux, nombre d'utilisateurs croissant, …), l'image d'Internet va se voir dégrader pour laisser place à « un média du piratage et de la pornographie » (Flichy, 2001) par les médias plus traditionnels que sont la presse, la télévision et la radio. Cette nouvelle description d'Internet constitue les prémices d'un terreau fertile à la naissance du cybercriminel et à ses premières représentations.

Si l'apparition d'Internet donne naissance au cybercriminel, les pirates des télécommunications, ce que restent généalogiquement les cybercriminels aujourd'hui, ne sont pas un phénomène nouveau. Les pirates des télécommunications sont devenus des cybercriminels car leur champ d'action a évolué avec les possibilités offertes par la technologie Internet, possibilités qui n'existaient tout simplement pas avec des outils de communication antérieurs. Nicolas Arpagian rappelle quelques faits historiques significatifs : « […] la France s'est dotée dès 1915 d'une Section de contrôle télégraphique afin d'inspecter les correspondances postales et télégraphiques en provenance, à destination ou transitant par son territoire. Quant aux pirates du téléphone, ils comment à sévir dès les années 1960. […] *Les blue boxes*, ces boitiers électroniques permettant de stopper la facturation des télécommunications à l'insu des opérateurs ont longtemps été le cauchemar des compagnies de téléphone étatsuniennes » (Arpagian, 2018 : 12).

1.1.2. Le contexte de la contre-culture

La contre-culture américaine des années 1960 joue également un rôle capital dans la démocratisation et le développement d'Internet en inspirant les fondateurs. La jeunesse se rebelle contre le système et souhaite lutter face aux décisions qu'elle juge injuste : racisme, centralisation excessive de certains capitaux au profit de grandes entreprises et de l'armée, guerre, …

Le mouvement hippie, qui est surement le plus emblématique et connu de cette période va regrouper bon nombre de jeunes étudiants qui participent activement à la création d'Internet dans leurs universités ou au travers de groupes de passionnés en informatique. Le mouvement ayant pour pilier fondamental l'aspect communautaire ainsi que le partage des connaissances (que l'on retrouve dans les communautés virtuelles des années 1980, vue précédemment), cette idéologie va profondément s'ancrer dans Internet. Dominique Cardon évoque d'ailleurs : « l'atmosphère culturelle qui nimbe la baie de San Francisco a profondément influencé la manière dont les premiers usagers de l'Internet se sont représentés l'outil qu'il étaient en train d'inventer » (Cardon, 2010).

Internet étant potentiellement vu comme un nouvel espace ou la prise de parole est autorisée avec peu, voir aucune contrainte, cette nouvelle technologie prometteuse est perçue comme une réelle opportunité et son développement s'en trouve nourri en conséquence. Face à cela, on remarque deux types de comportements : ceux qui veulent s'exprimer contre le gouvernement et les grandes entreprises directement par ce nouveau biais (poursuivre un combat) et ceux qui aspirent à vivre dans un monde à part, couper de la réalité des géants tels que la marque IBM qui symbolise le mal.

1.1.3. Le tournant du Web

En 2005, les principes d'Internet marquent un nouveau tournant en évoluant avec l'arrivée du Web 2.0 ou Web communautaire. Le Web 2.0 est profondément marqué par l'ère des communautés et l'importance accordée à l'internaute car il voit l'apparition de multiples plateformes sociales (Wikipédia, les outils de travail collaboratif, …) dont les réseaux sociaux (Facebook, Twitter, …) qui mettent au centre des attentions la communication entre individus et la production de contenus en collaboration. Les outils de publication se diversifient, de même que les besoins remplis par ses multiples plateformes (rencontre, enjeux professionnels, …). L'ubérisation des services[3] quelques années plus tard est aussi un évènement clé qui découle directement du Web 2.0. Benoît Dupont et Vincent Gautrais étoffent davantage les apports du Web 2.0.

> *Il importe de souligner la vigueur de la connectivité, de l'interactivité, encore une fois qui sont intensifiés avec le Web 2.0. Il est donc désormais possible de se connecter à l'autre facilement en adhérant aux plateformes des personnes qui nous intéressent, souvent appelées des 'amis'. Les outils qui se rangent en effet sous cette appellation, grâce à une flexibilité et une simplicité remarquables, favorisent l'interopérabilité des langages technologiques et, en fin de compte, des manières de s'approprier les contenus mis en ligne par autrui. L'information est donc beaucoup plus facilement poussée – et non pas seulement prise – vers d'autres (comme par le biais notamment de la syndication) ; l'information est aussi plus dynamique, les contenus pouvant être désormais appropriés et modifiés par une autre personne que celle qui en disposa en premier.*
>
> *(Dupont et Gautrais, 2010 : 4)*

[3] *cf.* Glossaire

En outre, ils utilisent l'expression « l'importance du 'You' » pour qualifier la place prépondérante qu'occupe l'internaute dans cette nouvelle génération du Web : « L'internaute qui consomme, mais surtout, ce qui est plus nouveau, qui alimente le contenu que l'on trouve sur les plateformes, dans les blogues et les wikis, permet la mise à disposition de contenus qui étaient habituellement l'apanage d'entreprises dédiées à ces contenus […]. Des contenus qui de surcroît, disposent de qualités nouvelles suffisamment significatives pour porter concurrence à cette même industrie » (Dupont et Gautrais, 2010 : 5).

Tout comme la génération précédente du Web, le Web 2.0 offre de nouvelles possibilités pour l'internaute, nouvelles possibilités qui se voient également appropriées et détournées par le milieu cybercriminel et favorisant les délits (cyberharcèlement, escroquerie, …). L'arrivée de fonctionnalités toujours plus performantes sur les interfaces Web entretient également les représentations autour du cybercriminel et de son champ d'action. Un fait spécifiquement questionnable qui constitue pourtant la logique des médias sociaux est à relever : « Le ressort des dynamiques expressives sur le Web est que, pour élargir leur espace relationnel, les internautes doivent aussi élargir la surface identitaire qu'ils exposent » (Cardon, 2010 : 66). Parmi d'autres, cette caractéristique est une porte ouverte bien présente dans les stratégies cybercriminelles que le Web 2.0 rend malheureusement possible.

1.2. La complexité du terme

Dans cette partie, nous abordons l'acte cybercriminel et observons par rapport aux recherches menées à ce jour ce qui est finalement entendu sous ce terme. Nous rendons compte de ce qui caractérise le cybercriminel, tantôt dans son comportement que dans son mode d'organisation ainsi que les difficultés de définition qui sont à relever. L'objectif de cette étape est de pouvoir confronter l'imaginaire, la représentation, à ce qu'il en est réellement de par ce qui se dégage du domaine de la recherche.

1.2.1. Un terme controversé

Les *hackers, hacktivistes* et autres collectifs font l'objet d'une partie dédiée dans ce présent état de l'art puisque la notion fait encore aujourd'hui l'objet de controverse. Des chercheurs et scientifiques de différents horizons (Sciences de l'Information et de la Communication, Criminologie, Psychologie, Informatique) considèrent les *hackers* comme des cybercriminels à à part entière alors que d'autres préfèrent conserver le sens historique de la notion. Le sens historique étant celui d'individus non criminels qui se passionnent pour l'informatique et

innovent grâce à des détournements techniques. Dominique Cardon conserve ce sens historique avec « un terme qui caractérise leur ingéniosité technique (et non, comme on l'entend parfois, une volonté malfaisante) » (Cardon, 2010 : 15). Tandis que d'autres comme Frédéric-Jérôme Pansier, tout en rappelant l'origine historique du terme, s'identifient à une signification criminelle : « Est alors offert aux hackers, un moyen d'action privilégié pour pénétrer de nouveaux systèmes, une opportunité de multiplier leurs connexions criminelles […] » (Pansier et Jez, 2000). Nous rappelons donc, par des étapes distinctes, le long processus qui encadre cette notion.

Au départ, les *hackers* ne sont pas des cybercriminels ou des pirates comme souvent assimilé aujourd'hui dans les discours médiatiques qui entourent nos sociétés contemporaines et parmi les actes produits de ceux qui s'y revendiquent. Cependant, la signification associée aux *hackers* s'est vue modifiée dans le temps, de même que pour les types d'actions qu'ils réalisent (apparition de statuts en fonction des actions menées : *black hat, white hat,* …) comme nous allons le voir.

Historiquement, le terme de « *hack* » signifie le fait de contourner, d'adapter un système à un besoin auquel il n'était pas forcément destiné. Ainsi, le seul terrain qu'est l'informatique pour uniquement user de ce terme est erroné. Ceux qui *hackent* sont ceux qui rusent en outrepassant les règles de conception techniques pour répondre à un besoin : « […] 'to hack', qui désigne le fait de parvenir au résultat désiré par des manipulations originales, nouvelles, voire encore largement inexpliquées » (Dagiral, 2008 : 484). Des connaissances issues de différents domaines peuvent nourrir cet acte nouveau. Les premiers hippies qui redoublent d'inventivité pour, par exemple, réaliser un système d'irrigation économe sur leurs plantations sont déjà, en soi, des *hackers* au sens originel du terme. La notion va ensuite puiser la source technologique qu'on la lui connaît parmi les passionnées de programmation de la première heure qui vont sans cesse chercher à réaliser de nouvelles prouesses. Éric Dagiral reconnait deux contextes d'origine des *hackers* : « celui du monde universitaire américain d'une part, et celui des clubs d'amateurs de technique d'autre part » (Dagiral, 2008 : 482). Les étudiants les plus animés par cette nouvelle technologie souhaitent la modifier pour leur envies personnelles avec au fond « l'idée et le désir de sa diffusion au plus grand nombre » (Dagiral, 2008 : 483). Comme nous pouvons le constater être *hacker* n'est en aucun cas quelque chose de péjoratif au commencement, cela est même, bien au contraire, synonyme d'une forme d'intelligence.

Parallèlement, nous pouvons énoncer le phénomène du *Growth hacking*[4] (littéralement traduisible par « pirate de croissance ») apparu en 2010 qui reprend la notion et qui signifie l'acte d'augmenter, par différents canaux numériques, l'activité d'une petite entreprise, le plus souvent de type *start-up*. À aucun moment cette nouvelle activité devenue une profession appartenant pleinement aux métiers du numérique n'est d'ordre criminelle.

Être *hacker*, c'est suivre l'éthique *hacker* qui s'entremêle avec celle de la contre-culture et se voit doter de grands principes : défiance de l'autorité, les informations sont des biens libres, … Aujourd'hui, cette éthique se révèle proche de la cybercriminalité. Des principes qui ne rentrent pas toujours en concordance avec la législation de la société réelle, ce qui pousse à considérer le Web comme un monde à part pour certains. C'est le cas à cette période où les premiers *hackers* apparaissent.

Par analogie, Peter Grabosky part de la relation entre le crime traditionnel et le crime produit en ligne pour définir ce qui est propre à la cybercriminalité. Dans un premier temps, les corrélations sont à présenter succinctement. Le crime en ligne dans sa manière de fonctionner n'a rien de nouveau puisqu'il repose sur trois piliers qui sont sensiblement les mêmes que pour le « *street crime* » ou crime terrestre : la motivation, l'opportunité et l'absence de gardien (Grabosky, 2001 : 248). Le crime en ligne facilite ses trois fondements pour les individus malintentionnés mais n'en ajoute absolument aucun : la motivation reste ce qu'elle est (« *the desire to taste 'forbidden fruit'* », *curiosity*, …), l'opportunité ne devient que plus grande et l'absence de gardien est concrète. « […] *motives for computer-related crime are nothing new. Technologies may change rapidly, but human nature does not* » (Grabosky, 2001 : 248). Pour Peter Grabosky, le crime en ligne se qualifie par deux principales nouveautés apportées par le changement de support : l'atteinte significative à l'intimité et les implications transnationales que permettent les nouvelles technologies. La quantité de données personnelles qui sont récoltées et produites par les réseaux sociaux ainsi que d'autres plateformes, les entreprises qui se vendent des données personnelles de clients à des fins marketings en passant par des structures décentralisées ; toutes ces actions banalisent l'accès à l'information personnelle. En s'appuyant sur d'autres travaux (ceux de Roger Clarke), Peter Grabosky mentionne que dans le passé, les informations personnelles étaient protégées par la dispersion des données mais avec Internet et l'arrivée du commerce en ligne, les données sont beaucoup mieux centralisées grâce aux bases de données notamment (Grabosky, 2001). Les implications transnationales

[4] https://fr.wikipedia.org/wiki/Growth_hacking

caractérisent également la cybercriminalité car il est possible pour un individu seul ou un groupe d'individus d'attaquer des serveurs se situant à des milliers de kilomètres. De surcroît, la législation n'est pas la même dans chaque pays ce qui encourage la coopération entre cybercriminels éloignés géographiquement et les attaques vers un état étranger à celui où le(s) cybercriminel(s) réside(nt). Un crime commis en ligne peut ne pas être répréhensible dans un pays ou avoir amplement moins d'importance dans celui-ci.

À cela, Bilel Benbouzid et Daniel Ventre optent pour une méthodologie d'analyse semblable à Peter Grabosky pour comprendre ce qu'est le cybercrime, « il faut d'abord se demander dans quelle mesure les 'cybercrimes' se différencient des autres activités que nous reconnaissons comme des crimes » (Benbouzid et Ventre, 2016 : 10). Ils font état d'une certaine difficulté à saisir le cybercrime qui découle d'une hétérogénéité de définitions « selon l'endroit où l'on place le curseur dans ce continuum de crimes liés par leur degré de dépendance à Internet » (Benbouzid et Ventre, 2016 : 11). Il existe des définitions en fonction que le crime se réalise sur un ordinateur contre un ordinateur, sur un ordinateur en extension d'un crime terrestre, … Des définitions s'englobent les unes dans les autres rendant la compréhension difficile. Néanmoins, les deux auteurs s'accordent à dire qu'il faut prendre l'acte cybercriminel dans sa globalité comme un assemblage entre crime et Internet, les deux pôles influant plus ou moins l'un dans l'autre (Benbouzid et Ventre, 2016 : 11).

Dans la continuité de sa pensée, Peter Grabosky poursuit avec l'illusion d'anonymat qui découle de la nouvelle manière d'envisager les relations interpersonnelles sur Internet. Cette recherche sur la notion d'anonymat délimite les possibilités techniques concevables pour le cybercrime, elle nous renseigne sur la posture du cybercriminel en plus de nous éclairer sur la représentation. « *The illusion of anonymity seems to have elicited more candour over the internet than one would expect in face-to-face communications* » (Grabosky, 2001 : 244). Depuis Internet, chacun peut jouer un rôle plus facilement en se retranchant derrière un masque avec l'utilisation de pseudonymes, tandis que dans le monde réel, cela est bien moins aisé. La tentation de se faire passer pour quelqu'un d'autre ou d'agir différemment est plus forte. Cette illusion d'anonymat s'incorpore pleinement à la représentation du cybercriminel comme peut en témoigner le résultat sous-jacent de cette recherche Google pour le mot clé « cybercriminel » (*cf.* Figure 3, page 37).

L'anonymat et la traçabilité des informations jouent un rôle prépondérant dans l'acte cybercriminel. Marc Ouimet ne manque pas de souligner ce facteur en développant que

« pratiquement toute action peut être retracée ; l'anonymat d'Internet est donc un mythe » (Ouimet, 2006 : 16). Il rejoint l'illusion d'anonymat nommée par Peter Grabosky. Si les cybercriminels les plus avertis usent de moyens techniques pour contrer cette traçabilité en se créant un anonymat plus convaincant avec l'utilisation du navigateur Tor [5]par exemple, l'accès à Internet par VPN[6] ou l'usage de la cryptographie (logiciel PGP[7], …) que nous allons développer, une enquête minutieuse permet toujours de remonter à la source. Marc Ouimet spécifie de façon additionnelle que ces préconisations prises par ces cybercriminels ne concernent qu'une faible partie d'entre eux (Ouimet, 2006). En outre, bien que certaines données sont complexes à collecter et nécessitent un temps considérable, d'autres vecteurs comme les transactions financières sont une source d'information. Chaque dispositif utilisé (sites, plateformes, logiciels) par le cybercriminel génère des données : il y a par conséquent une grande pluralité de sources existantes. « Il faut un utilisateur hyper-consciencieux pour ne pas commettre d'erreur […]. […] Lorsqu'on décide d'utiliser Internet, on accepte d'être repérable » (Ouimet, 2006 : 16).

La traçabilité sur Internet est à la fois une protection mais aussi une arme qui permet de borner différents types d'attaques cybercriminelles. Cette traçabilité en tant qu'arme est constitutive de certaines attaques cybercriminelles. L'espionnage, le cyberharcèlement sont des actes cybercriminels qui reposent sur la traçabilité de l'information. Ils ne nécessitent d'ailleurs pas nécessairement de connaissances techniques poussées mais juste des recherches sur les réseaux sociaux, sur les sites d'entreprises, ...

Enfin, Peter Grabosky termine par l'arrivée du commerce en ligne qui a apporté la cryptographie, véritable « *boon* » pour les cybercriminels (Grabosky, 2001 : 246). La cryptographie est la base de tout échange commercial en ligne : c'est le fait de crypter des données. Elle se traduit par la faculté à les rendre illisibles pour certains si ceux-ci ne disposent pas de la clé de déchiffrement. La cryptographie est le socle d'une partie des actes qualifiables de cybercriminels car elle permet de réaliser des transactions, de s'approprier des informations, de faire transiter des contenus. Elle rend l'acte cybercriminel possible, durable (génération de bénéfices) et le caractérise. Les rançongiciels[8] (*ransomwares*) sont des attaques

[5] Tor est un réseau informatique superposé mondial et décentralisé (Source : *Wikipédia*).
[6] *Virtual Private Network*, un réseau privé virtuel offre la possibilité de se connecter à Internet en masquant certaines de ses informations selon différents critères.
[7] *Pretty Good Privacy*, logiciel de chiffrement cryptographique.
[8] *cf.* Glossaire

cybercriminelles usant de la cryptographie à des fins malveillantes, ils confisquent des fichiers à leur propriétaire légitime, nous étudierons ce cas avec la disquette Sida (Casilli, 2015).

Ce mode d'échange de l'information génère très largement la représentation du cybercriminel en plus de définir l'acte en faisant partie de son fonctionnement. C'est ainsi que nous la retrouvons dans la représentation du cybercriminel sous formes de « chutes de données », de lignes binaires incompréhensibles. Son illustration provient également de l'imaginaire collectif largement inspiré de la série cinématographique *Matrix* qui met en scène la *Matrice* (simulation de la réalité où les humains sont emprisonnés) par cette même forme de « chute de données ». Tout comme le pied-de-biche est l'un des outils du criminel terrestre, la cryptographie est l'une des clés du cybercriminel.

Figure 1 : la Matrice illustrée dans Matrix (Source : Google Images)

Internet est le territoire d'action de la cybercriminalité. L'environnement change logiquement les paramètres d'études poussant à définir ce qu'est l'acte cybercriminel. Il en va de même pour les perceptions des acteurs qui agissent dans cette espace (internautes, entreprises, …). La dématérialisation des biens a un impact notable en faussant la vision du contexte. Les difficultés à fixer l'acte cybercriminel s'en sont trouvées renforcées.

> *Le concept tente de produire une cassure radicale entre l'usage encouragé et l'usage possible qui, dans le cyberespace, n'existe tout simplement pas. Dans l'espace traditionnel, il est facile de voir une différence entre un objet gratuit, ou abandonné, […]. Dans l'espace virtuel, il faut revoir entièrement la notion d'opportunité criminelle : dans un environnement où la notion de propriété se rapporte exclusivement à de l'information, copiée, échangée, modifiée, l'opportunité criminelle n'est plus rien d'autre que le revers de l'opportunité commerciale.*
>
> *(Leman-Langlois, 2006)*

Par ailleurs, Stéphane Leman-Langlois justifie d'une seconde raison cette complexité de l'objet cybercriminalité ; elle est la conséquence de la multiplicité des acteurs qui entrent en jeu. Ces acteurs manient la notion avec beaucoup de libertés en complément d'« une mauvaise compréhension du fonctionnement et des possibilités de l'informatique réseautée » (Leman-Langlois, 2006 : 78).

En droit, pour qualifier un cybercrime et mettre en cause des responsables, des problématiques se posent avec Internet. Frédérice-Jérome Pansier et Emmanuel Jez rappellent d'abord que « le vide juridique n'est qu'un mythe », des lois existent déjà comme celles valables pour l'audiovisuel, le droit de la presse, … La difficulté réside dans l'adaptation de ses lois à Internet (Pansier et Jez, 2000 : 4). À commencer par les implications transnationales qui ont complexifiées les procédés. La collaboration entre états est inévitable pour adopter des solutions efficaces face au crime en ligne et être sûr que chaque nation est en accord commun avec ce qui est entendu par le vocable cybercrime. Seulement, ces collaborations ne sont pas simples à mettre en place ce qui rallonge fortement les délais de traitement. Il s'ajoute à cela une redéfinition du droit de la preuve découlant de l'information dématérialisée : il s'agit de savoir comment prouver qu'un acte cybercriminel est commis. En second lieu, le « jeu des responsabilités » ou la responsabilité pénale est un sujet épineux puisque les crimes en ligne font appel à différents intermédiaires (Pansier et Jez, 2000 : 11). Certaines entreprises proposent des solutions logicielles qui dépendent parfois d'une autre juridiction, elles sont alors amenées à refuser la cession d'informations aux autorités étrangères. Par exemple, pour le partage de fichiers illégaux, ces fichiers sont souvent hébergés sur des sites intermédiaires spécialisés qui se dédouanent de certaines responsabilités. Les Fournisseurs d'Accès Internet (FAI) occupent aussi une position délicate vis-à-vis de la cybercriminalité sur des questions de responsabilité comparables. Frédéric-Jérôme Pansier et Emmanuel Jez définissent la cybercriminalité de la façon suivante : « phénomène criminel radicalement nouveau dans lequel l'ordinateur apparaît comme la cible privilégiée par le délinquant » (Pansier et Jez, 2000 : 12). On se situe dans une posture tout à fait dissemblable de ce que nous avons pu voir jusqu'à présent sur ce qui est déterminé par le terme cybercrime.

À l'heure actuelle, les solutions législatives pour délimiter la cybercriminalité sont encore en cours d'élaboration. L'Union européenne et les pays qui la composent comme la France tiennent une bonne posture en créant et soutenant des infrastructures, des unités spécialisées

(ANSSI[9], BEFTI[10], EC3[11], …). La législation progresse également au cas par cas, ce n'est qu'avec la poursuite en justice d'affaires concrètes que la situation s'améliorera.

Bien que des délimitations du cybercrime et du cybercriminel soient encore floues sur certains aspects, il n'en reste pas moins que les « règles » implicites d'Internet (règles de bonne conduite, savoir-vivre) sont suivies par tous les individus présents sur le réseau depuis son commencement (Flichy, 2001 : 124). Le cybercriminel est avant tout un internaute qui fait le choix d'adopter une attitude non éthique et son action s'inscrit dans ce même écosystème qu'est Internet. Patrice Flichy parle de « l'utilisateur déviant », de « comportements déviants » pour ceux qui s'adonnent à des actions qui « perturbent le fonctionnement normal d'une partie du réseau ». Par ces actes, Patrice Flichy cite Ed Krol dans l'ouvrage *Le Monde Internet* publié en 1994 précisant : « le harcèlement et les comportements haineux ou asociaux, les dommages intentionnels ou la perturbation des autres utilisateurs, la mise en accès public de fichiers obscènes » (Flichy, 2001 : 124). Nous en apprenons déjà plus sur ce qui constitue les prémices des actes cybercriminels.

« Les internautes pratiquent donc l'autodiscipline » (Flichy, 2001 : 124). Cette mécanique s'observe également chez les groupes de cybercriminels et permet de les définir plus distinctement par leur mode d'organisation. Les groupes cybercriminels (APT41[12], TA505[13], …) dont une partie d'entre eux proposent de monnayer leurs services. Nous étofferons ce propos avec plus de précisions.

1.2.2. Les types

À ce sujet qu'est le cybercrime, des chercheurs se focalisent sur la création de typologies. Les objectifs de ses différentes classifications visent à améliorer la compréhension de ce qui distingue l'acte cybercriminel, le cybercriminel en tant qu'individu, ... On retrouve plusieurs catégorisations scientifiques reflétant la pluralité de travaux provenant de la criminologie, de la psychologie, de la sociologie, du droit et d'autres disciplines. Elles apportent chacune un sens spécifique qu'il est pertinent de présenter puisqu'elles nous éclairent dans ce présent travail.

[9] Agence Nationale de la Sécurité des Systèmes d'Information
[10] Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information
[11] *European Cybercrime Centre*
[12] https://www.theguardian.com/technology/2019/aug/08/chinese-cyberhackers-blurring-line-between-state-power-and
[13] https://www.francebleu.fr/infos/faits-divers-justice/attaque-informatique-au-chu-de-rouen-un-groupe-de-pirates-particulierement-actif-en-france-1574961722

Bilel Benbouzid et Daniel Ventre s'accordent à définir sociologiquement le « crime en ligne » selon trois sections distinctes à partir de recherches dirigées par David S. Wall (criminologue anglais et ancien directeur de l'École en Sciences Sociales Appliquées). Ils classent : « le crime assisté par ordinateur (*cyber-assisted crime*) », « le crime facilité par internet (*cyber-enabled crime*) » et « le crime dépendant d'Internet (*cyber-dependant crime*) » (Benbouzid et Ventre, 2016 : 11). Tout acte cybercriminel appartient à une de ces sections. Dans le premier cas « le crime persiste en retirant Internet », dans le second « le crime ne disparait pas si on retire Internet, mais change de dimension en passant du global au local » et dans le troisième « le crime disparaît complètement en retirant Internet » (Benbouzid et Ventre, 2016 : 11). On retrouve dans les crimes assistés par ordinateur : le cyberharcèlement, l'ingénierie sociale, le trafic de cartes de crédits (*carding*), l'usurpation d'identité, le détournement de fonds, … Parmi les crimes facilités par Internet, sont classées toutes les attaques dépendant d'un large partage tel que les spams, les logiciels malveillants, la mise en ligne de fichiers illégaux, … En dernier point, les attaques par hameçonnage (*phishing*) avec la création de sites Web usurpant l'identité d'institutions de confiance, les attaques serveurs par surcharge de requêtes (DOS pour *Denial Of Service attack*), le *mailbombing* (blocages de messageries électroniques grâce à une saturation d'envois), les intrusions informatiques ; toutes ses actions appartiennent aux crimes dépendants d'Internet (Benbouzid et Ventre, 2016 : 11).

Frédéric-Jérome Pansier et Emmanuel Jez divisent dichotomiquement le crime en ligne : il y a les crimes qui visent les ordinateurs et les crimes qui sont l' « outil d'un crime conventionnel » (Pansier et Jez, 2000). Pour les auteurs, la cybercriminalité correspond à la première catégorie. Le marquage est fait par rapport à l'usage du support informatique.

Ils nomment l'acte cybercriminel ciblant les systèmes informatiques par « attaque logique ». Les attaques logiques peuvent être effectuées à distance mais aussi physiquement, nous pensons à l'utilisation d'une clé USB par exemple. Deux types d'attaques logiques ou d'actes cybercriminels sont répertoriés : les « agressions directes » et les « agressions indirectes » (Pansier et Jez, 2000 : 105). Les agressions directes se composent des intrusions, du *mailbombing* et des bombes logiques (programmes qui détruisent, sur commande du cybercriminel, des données et/ou du matériel informatique). Elles-mêmes comprennent le piratage par ligne téléphonique (*phreaking*), la communication avec l'ordinateur piraté et le piratage de mots de passe. Les agressions indirectes incluent quant à elles les virus (« programme ayant pour finalité d'altérer, d'endommager ou de détruire un système

informatique ») et les vers qu'ils traduisent par « un programme autoreproducteur propageant des copies de lui-même au travers du réseau » (Pansier et Jez, 2000 : 109).

Stéphane Leman-Langlois sépare les termes « crime par ordinateur » et « cybercrime ». Il tient à faire la différence entre ce qui est pour lui une notion trop générique dénuée de réel sens et le cybercrime qu'il définit par les « actes impliquant l'utilisation de réseaux informatisées, Internet principalement » (Leman-Langlois, 2006 : 66). Une posture critique est prise vis-à-vis du préfixe « cyber » au mot « crime » qui dépend plus d'un discours médiatique que d'une recherche approfondie. L'auteur fait ressortir des questions centrales déjà énoncées dans ce travail par d'autres chercheurs pour tenter de définir le cybercrime : « il semble utile de tenir compte du rôle des réseaux informatiques dans différentes formes de crimes. Dans certains cas, ils sont simplement accessoires à la commission d'un acte criminalisé, alors que dans d'autres, ils se trouvent au cœur même des activités visées, […] » (Leman-Langlois, 2006 : 66).

En résultat de ses recherches, Stéphane Leman-Langlois dresse ce tableau (*cf*. Tableau 1), typologie de la cybercriminalité.

Réseaux/cyberespace ont un rôle :	incrimination des actes	
	traditionnelle (préInternet)	émergente/imminente (postInternet)
Déclencheur	(non applicable)	attaques distribuées ; vandalisme virtuel
Multiplicateur	pornographie juvénile ; vol d'identité ; fraudes ; incitation à la haine	échange de fichiers ; pourriels
Accessoire	appâter des victimes ; terrorisme et sabotage	terrorisme (support)

Tableau 1 : la cybercriminalité en fonction des incriminations et de l'influence des réseaux (Source : Leman-Langlois, 2006)

On constate la présence des attaques distribuées, du « vandalisme virtuel », de la pornographie juvénile, de l'échange de fichiers, … Stéphane Leman-Langlois prouve par plusieurs exemples et avec l'appui d'informations chiffrées la présence des « crimes traditionnels dans le monde virtuel » ainsi que « la création de nouvelles formes de criminalité ». Le partage de fichiers musicaux est un acte préexistant (préInternet) mais Internet donne une impulsion qui affecte l'industrie musicale au point de rendre cette activité répréhensible (Leman-Langlois, 2006 : 68). Le partage de fichiers musicaux ou de toutes œuvres culturelles sans autorisation préalable est un acte cybercriminel. Concernant les nouvelles formes de criminalité, l'auteur identifie le

« vandalisme virtuel » que l'on appelle aussi plus couramment défacement. Cette pratique consiste à pénétrer illégalement dans un serveur Web afin de changer l'aspect visuel du site internet en question, une atteinte à l'image 2.0 ou atteinte à l'e-réputation.

En dernier protocole recensé, s'intéresser aux conséquences des attaques cybercriminelles aide à mieux en spécifier les types. Cette dernière approche de la cybercriminalité par le risque est réalisée par les chercheurs pour identifier les types d'actes cybercriminels.

En premier lieu, Nicolas Arpagian expose deux familles d'attaques informatiques existantes sur lesquelles reposent des faits historiques tels que l'affaire Stuxnet[14], WannaCry[15], … (Arpagian, 2018). Ces cyberattaques sont ou non d'ordre criminel au regard de qui en est la source. Tout d'abord, il identifie les « attaques sur les réseaux informatiques et téléphoniques » : celles-ci prennent en compte l'espionnage, l'altération de données et la prise de contrôle total à distance. Ensuite, les « attaques informationnelles » dont font partie l'atteinte à l'e-reputation et le commerce illégal. Aux termes de ses recherches, l'auteur classifie quatre conséquences des cyberattaques qui sont les finalités souhaitées par les cybercriminels : « les conséquences pour l'environnement, les conséquences économiques, les conséquences politiques et les conséquences liées au cumul et à la combinaison des circonstances » (Arpagian, 2018 : 44).

Sur l'appui d'un échantillon de comportements comprenant 195 cas collectés rigoureusement du 6 octobre 2008 au 15 avril 2009, Benoît Dupont et Vincent Gautrais se concentrent sur les risques liés au Web 2.0 dans la finalité de dresser une typologie des « comportements criminels et déviants » existants en ligne (Dupont et Gautrais, 2010 : 11). Générée depuis un agrégateur de contenus numériques, leur base de données formule les résultats suivants qu'ils classifient par rubriques dans un tableau (*cf.* Tableau 2).

[14] https://www.franceculture.fr/emissions/la-methode-scientifique/la-methode-scientifique-emission-du-mercredi-05-fevrier-2020
[15] https://www.lemonde.fr/pixels/article/2017/05/13/ce-que-l-on-sait-du-logiciel-de-racket-qui-a-paralyse-les-hopitaux-britanniques-et-touche-des-dizaines-de-pays_5127351_4408996.html

Type de risques	Type de comportement	Fréquence	Pourcentage
Risques criminels (atteintes aux personnes)	Crime sexuel	68	34,9
	Violence physique	17	8,7
	Harcèlement et menaces	17	8,7
Risques criminels (atteintes aux biens)	Attaque informatique	33	16,9
	Fraude	16	8,2
Risques réputationnels	Contenu problématique	35	17,9
	Autre	9	4,7
	Total	195	100

Tableau 2 : distribution des cas par type de risques (Source : Dupont et Gautrais, 2010)

Après examen des résultats, les deux auteurs répertorient deux types d'actes cybercriminels : les actes cybercriminels visant les personnes et les actes cybercriminels visant les biens. Les risques réputationnels (*cf.* Tableau 2) ne dépendent pas de la criminalité en ligne selon leurs recherches mais « plutôt du droit civil et commercial » (Dupont et Gautrais, 2010 : 13). Par ce raisonnement, le « contenu problématique » (présent dans les risques réputationnels - *cf.* Tableau 2) qui intègre les menaces à l'intégrité de la vie privée et les menaces à la réputation des organisations ne constitue par un acte cybercriminel car toute notion de crime est écartée par les auteurs. Dans les actes cybercriminels portant atteintes aux personnes (*cf.* Tableau 2), nous retrouvons : le crime sexuel, la violence physique, le harcèlement et les menaces. Le crime sexuel et la violence physique se constituent d'échanges numériques ayant donnés lieu à une rencontre réelle entre les partis ; le crime sexuel comporte également l'envoi de fichiers pédopornographiques. Dans les cybercrimes portant atteintes aux biens, Benoît Dupont et Vincent Gautrais notifient l'attaque informatique (tous types de logiciels malveillants confondus) et la fraude (les vols d'identités servant l'ingénierie sociale).

Pour conclure sur les typologies existantes du cybercrime, Solange Ghernaouti et Arnaud Dufour qualifie la cybercriminalité par « toutes les activités criminelles réalisées au travers du cyberespace et en particulier du réseau Internet » (Ghernaouti et Dufour, 2017 : 101). Nous apercevons la dimension supplémentaire adoptée par les auteurs qui séparent spatialement Internet et cyberespace. Les deux scientifiques marquent la cybercriminalité suivant deux attributions faites des TIC : en tant que cibles (vols de données, intrusions, destruction, …) et en tant que moyen (outils et armes). « Les délits perpétrés peuvent-être classiques […] ou propres aux technologies » (Ghernaouti et Dufour, 2017 : 102). La cybercriminalité se constitue de quatre éléments qui diminuent la prise de risque des cybercriminels : « la dématérialisation

des services et transactions, l'usage de fausses identités ou d'identités usurpées, le nombre d'intermédiaires techniques, le recours à des techniques permettant de masquer l'origine des attaques » (Ghernaouti et Dufour, 2017 : 102). On rejoint le contexte complexe qu'a instauré le cyberespace avec l'opportunité criminelle que Stéphane Leman-Langlois présente, opportunité criminelle qui s'accroît avec la réduction des prises de risque des cybercriminels argumentée par Solange Ghernaouti et Arnaud Dufour.

Un dernier acte cybercriminel est à présenter, celui-ci génère une dimension fictive non négligeable pour le cybercriminel car il est sujet à de nombreuses discussions et à une forte médiatisation issue de tous bords. Benoît Dupont y consacre une étude complète afin de bien en comprendre le fonctionnement et l'incidence. Cet acte cybercriminel n'est autre qu'un moyen frauduleux qui permet d'exécuter une variété importante de cyberattaques (DOS, hameçonnage, pourriels, …) telles que nous les avons étudiés dans les typologies faites par les chercheurs : l'utilisation de *botnets* ou de « machines zombies ». L'auteur en donne la définition suivante : « un botnet est un ensemble de machines informatiques contrôlées à l'insu de leur propriétaire légitime par un pirate informatique qui les utilise de manière coordonnée » (Dupont, 2014 : 181). L'usage de *botnets* par les cybercriminels alimente cette idée que le cybercriminel est « partout », qu'il peut frapper quand il le veut, où il le souhaite et par-dessus tout avec une puissance de calcul dépassant toutes les attentes (l'ensemble sans se faire démasquer). Le cybercriminel maîtriserait l'ubiquité imaginaire d'Internet. Les cybercrimes officiés par l'intermédiaire de *botnets* sont les attaques cybercriminelles les plus abouties en terme d'organisation, Benoit Dupont parle d'une « industrialisation des processus » (Dupont, 2014 : 181). En effet, c'est à l'aide de *botnets* que les serveurs de grandes organisations sont surchargés jusqu'à les rendre inaccessibles, que des millions de pourriels sont envoyés massivement chaque jour dans les messageries électroniques de particuliers, ...

Nicolas Arpagian rappelle une spécificité des *botnets* dans son ouvrage : « […] le fait de localiser les ordinateurs d'où sont parties les attaques ne signifie pas que ceux-ci aient été utilisés avec l'accord de leur propriétaires légitimes ou l'assentiment des autorités de l'État en question » (Arpagian, 2018). Une cyberattaque menée par ce moyen provient d'une multitude de positions géographiques à un même instant, en ce sens, ce type d'attaque est profondément internationalisé. Il y a une part de vérité existante dans la représentation du cybercriminel qui contrôlerait l'ubiquité mais cette figure reste toutefois hyperbolique.

Nous examinons donc la grande disparité de définitions et typologies qui tentent d'encadrer le cybercrime et le cybercriminel. Des chercheurs considèrent que la cybercriminalité est uniquement composée par les attaques à destination des biens alors que d'autres chercheurs ne raisonnent pas de cette manière. D'autres chercheurs se focalisent davantage sur le rôle qu'occupent les machines informatiques quand d'autres réfléchissent sur la diversité des répercussions recensées. De même, la multiplicité des attaques dénombrées et identifiées à ce jour ne permet toujours pas une classification précise à laquelle tous les scientifiques se rattachent. Nous pouvons justifier ce diagnostic par : l'effectif toujours croissant d'internautes arrivant sur le réseau des réseaux, le développement de la cybercriminalité et de ses attaques suivant la vitesse fulgurante du développement des TIC, le bruit généré par tous les acteurs de nos sociétés contemporaines (entreprises, médias, institutions étatiques, …). Tous ces facteurs semblent avoir raison des démarches scientifiques.

1.2.3. *Hacker* et cybercriminel

Les modes d'organisation du cybercriminel témoignent de ce qui le caractérise. Les cybercriminels ont plusieurs méthodes d'action, les faits antérieurs s'étant produits historiquement rendent possible pour les chercheurs la collecte d'informations précieuses à ce sujet. Ces connaissances permettent de davantage définir le cybercriminel et son acte en posant des limites à ce qu'il est possible de faire ou non jusqu'à présent par l'intermédiaire des dynamiques de groupe.

Le cybercriminel n'agit pas uniquement seul, l'Histoire démontre le contraire. David S. Wall fait état de groupes cybercriminels qui agissent et qui ont existé pour mettre en évidence l'intérêt du mode d'action pour comprendre la cybercriminalité (Wall, 2015). Le chercheur s'appuie sur des cas recensés que sont Anonymous, LulzSec, Lizard Squad et d'autres en complément des écrits provenant de ses confrères. Pour exemple, LulzSec est spécifiquement connu pour avoir piraté des données appartenant à la multinationale japonaise Sony, pour la désactivation temporaire du site de la CIA et d'autres activités visant des organisations étatiques, des sociétés privées de renommée mondiale, … L'arrestation des membres du groupe en 2011 et 2012, l'accès aux échanges du groupe et la collaboration avec les autorités d'un des mis en cause rend concrète la compréhension du mode opératoire de ce groupe cybercriminel.

Le cybercriminel n'a plus besoin de compétences pratiques expertes pour mener à bien son action car toutes les actions tendent à être de nature automatisée (Wall, 2015). L'exemple des

rançongiciels et des *Rootkits*[16] est présenté par le chercheur car ils ont la capacité de s'auto-dissimuler dans les ordinateurs, tablettes, smartphones sans la moindre action de l'émetteur. L'auteur met en exergue l'expression « *Crimeware-as-a-Service* - CaaS » (en référence au modèle du *Cloud* « *Softare-as-a-Service* – SaaS »)[17] pour traiter ce comportement des cybercriminels. Nous nous éloignons de la représentation du cybercriminel surqualifié qui connaît toutes les spécificités de son langage informatique. David S. Wall emploie le terme de « *script-kiddie* » pour exprimer cette génération de cybercriminels aux compétences techniques restreintes qui se contentent de réutiliser les outils offensifs que d'autres cybercriminels conçoivent.

La logique des groupes cybercriminels s'articule sur la base de relations asymétriques qui ne sont que les effets produits par les médias sociaux et le Web 2.0 ; des spécificités largement argumentées par Dominique Cardon. En raison de ces relations, les cybercriminels s'organisent conformément à une idéologie, à des affinités, à de la notoriété. Les groupes cybercriminels sont ainsi particulièrement flexibles, éphémères et amorphes (Wall, 2015 : 78). À l'image du groupe Anonymous, les cybercriminels membres priorisent l'identité du collectif avant tout. Les cybercriminels se jugent par leurs actes et l'on retrouve en cette pratique une certaine empreinte de « *the old hacker ethic* » pour emprunter l'expression de David S. Wall. La réputation et la notoriété occupent une place spécifique dans la construction de l'identité du cybercriminel. Stéphane Leman-Langlois décrit un « goût de l'exploit », « c'est l'exploit en soi qui est visé, davantage que le gain » (Leman-Langlois, 2006 : 75). Il y a la « […] volonté d'obtenir une certaine reconnaissance sociale permettant de s'insérer et de se reconnaître dans un groupe » (Pansier et Jez, 2001). Les groupes cybercriminels suscitent un intérêt au travers de débats médiatiques et de l'imaginaire car ils diffèrent grandement du crime organisé traditionnel (Wall, 2015).

D'après ses trois études de cas et son recensement des groupes cybercriminels, David S. Wall rédige que les cybercriminels se rallient en groupe pour se spécialiser dans un type de cybercrime. L'auteur relate un assemblage, un modèle distribué (« *a distributed model of organised crime online* » - Wall, 2015 : 84) plutôt qu'une organisation pour définir le rassemblement de cybercriminels. Il rapporte que la structure des cybercriminels pratiquant leur activité en groupe est de nature décentralisée, finalement à l'image d'Internet. Le modèle

[16] *cf.* Glossaire
[17] *cf.* Glossaire

hiérarchique traditionnel ne s'établit pas, aucun cybercriminel n'est au-dessus d'un autre mais chacun réalise ses actions en adéquation à son savoir. « *Thus, cybercrimes and cybercriminals, by their very informationnal, networked and global nature go against the very grain of the traditionnal model of socially and geographically rooted organised crime models. […] cybercriminals evade control by traditionnal organised crime groups in much the same way as they evade control by, say, government* » (Wall, 2015 : 79). Ce passage est également cité par Bilel Benbouzid et Daniel Ventre dans leur sociologie du crime en ligne (Benbouzid et Ventre, 2016 : 15).

David S. Wall spécifie les coopérations entre cybercriminels avec plusieurs rôles que sont le « *Kingpin* » (marchand), le « *Broker* » (courtier) et d'autres afin de démontrer l'organisation des cybercriminels qui s'orientent sur le développement de logiciels malveillants (Wall, 2015 : 81). Les groupes cybercriminels collaborent avec d'autres intermédiaires cybercriminels et non cybercriminels pour compléter leur action. De plus, les individus d'un même groupe peuvent ne jamais être amenés à se rencontrer physiquement et être d'un lieu géographique tout à fait distinct (Wall, 2015). On marque ici certains points de concordances avec les recherches de Peter Grabosky par sa mise en avant des « implications transnationales » comme principale nouveauté de cette forme de criminalité d'un point de vue organisationnel.

Dans une étude scientifique sur la contrefaçon textile à l'ère de la cybercriminalité, les chercheurs Franck Guarnieri et Éric Przyswa soulèvent plusieurs questions sur la frontière entre la criminalité réelle et la cybercriminalité. Ils évoquent une « crise des frontières » provoquée par Internet qui se transcrit par une « interpénétration » entre le licite et l'illicite (Guarnieri et Przyswa, 2012 : 177). Au sein de leur réflexion sur la contrefaçon à l'ère du cybercrime, les deux scientifiques affirment que les groupes cybercriminels utilisent des entreprises déclarées légalement pour atteindre leur but, nous retournons sur les constats faisant ressortir les complexités des intermédiaires multiples. Dans ces cas de contrefaçon à la dimension cybercriminelle, le cybercriminel est aussi un « criminel en col blanc ». Des mécanismes de blanchiment sont effectués, des détournements financiers, des exploitations de « trous structuraux », … Cette imbrication fait écho au « crime commis par extension » (Pansier et Jez, 2000).

En allant plus loin dans un axe de recherche global et mondialisé, Solange Ghernaouti et Arnaud Dufour convoquent des éléments organisationnels qui soutiennent une véritable « économie du cybercrime » (Ghernaouti et Dufour, 2017 : 103). La cybercriminalité est un secteur à part

entière qui comporte ses propres marchés parallèles. Une partie de cybercriminels appartiennent à ce pôle en monnayant leurs services, leurs connaissances, leurs logiciels malveillants ou directement leurs produits illégaux (exemple du site Wall Street Market[18], …). C'est précisément par ces plateformes intermédiaires que les « *script-kiddies* » recherchent leurs outils pour passer à l'acte. La cybercriminalité s'est démocratisée et n'est plus uniquement l'activité d'une élite informatique.

En définitive, sur les différentes études conduites visant l'organisation du cybercriminel, on constate des modes opératoires protéiformes qui ne font que transposer la pluralité de comportements existants chez les cybercriminels. Il n'y a que plus de façons de définir un cybercriminel, entre jeunes « *script kiddies* » et experts informatiques confirmés.

Benoît Dupont et Vincent Gautrais prouvent par leurs lectures de rapports professionnels une exagération du secteur privé attisant l'insécurité (Dupont et Gautrais, 2010). Dans ce même travail, les auteurs démontrent que si la « prolifération des connaissances pseudo-scientifiques » des entreprises se réalise, c'est parce qu'il y a une absence de chiffres officiels fiables qui s'explique par une difficulté de quantification pour la cybercriminalité (Dupont et Gautrais, 2010 : 9). La cybercriminalité est laborieusement mesurable : il faut soit recenser toutes les attaques se produisant sur Internet à l'aide d'un outil qui n'existe tout simplement pas ou bien identifier toutes les victimes et recueillir leurs informations. Or, la cybercriminalité est profondément décentralisée, des tâches comme celles mentionnées ne peuvent être véritablement réalisables dans des conditions rigoureuses. Pourtant, Benoit Dupont relève la tentative des sondages de victimisation organisés au Québec en 2007 bien qu'ils restent toutefois très lacunaires et pour cause, les victimes ne souhaitent que rarement en parler aux organismes compétents. « […] les autres ne jugeant pas utile d'impliquer les autorités en raison d'un préjudice financier jugé négligeable, de leur satisfaction à l'égard des politiques de remboursement des institutions financières ou d'une méconnaissance des institutions pouvant leur venir en aide » (Dupont et Gautrais, 2010 : 9).

Bilel Benbouzid et Daniel Ventre déplorent également ce problème de quantification avec un « état des données disponibles […] encore très limité » (Benbouzid et Ventre, 2016 : 16). Pour leur part, ils expriment une sous-représentation : le nombre de plaintes enregistrées n'est pas du tout évocateur de l'impact réel de la cybercriminalité. « La nature globale, distribuée et

[18] https://www.france24.com/fr/20190506-darknet-wall-street-market-arrestation-drogue-arme-internet-supermarche

réticulaire du crime sur Internet rend impossible la centralisation nationale du comptage à partir d'un dispositif technique capable de saisir l'ensemble des infractions cybercriminelles » (Benbouzid et Ventre, 2016 : 16). Si un tel outil voit le jour, il met fin à l'une des plus grandes problématiques d'Internet : rendre possible une surveillance centralisée du réseau jamais égalée jusqu'alors (collecte et classification automatique de données numériques par type de cybercrime : adresses IP, code informatique, registres, …). Ils donnent toutefois l'exemple moins avancé mais existant des sites officiels de collecte d'URL[19] non sécurisés aux contenus douteux. Ce sont les internautes eux-mêmes qui viennent indiquer un signalement dans ces procédures. « Les enquêtes par questionnaire ne sont pas le seul moyen de produire de la connaissance sur le crime en ligne » (Benbouzid et Ventre, 2016 : 19), ils s'orientent donc vers des études plus numériques moins conventionnelles conformément à ce qui a été dit.

Les deux chercheurs mettent en lumière un autre facteur rendant ardu la quantification par les enquêtes de victimisation : le manque de connaissances des victimes. Elles ne savent pas toutes forcément identifier et expliciter clairement le type d'attaque à laquelle elles font face au moment de répondre à l'enquête. D'autre part, la captation de données depuis une échelle locale et non nationale pour une quantification du cybercrime semble être un bien meilleur moyen aux regards de Bilel Benbouzid et Daniel Ventre. Sur la base de données récoltées sur le terrain, en communication directe avec les concernés (données vérifiables et avérées) contrairement aux études d'entreprises commercialisant des logiciels antivirus et aux enquêtes publiques nationales, ces approches permettent d'endiguer l'imaginaire et les discours.

Anne-Marie Côté, Maxime Bérubé et Benoit Dupont développent en profondeur la quantification de la cybercriminalité par les organisations de sécurité en se basant sur l'analyse de treize rapports d'entreprises œuvrant dans la cybersécurité datés de 2014 (Côté, Bérubé et Dupont, 2016). La quantification hasardeuse de la cybercriminalité est la conséquence de quatre facteurs :

- « L'absence de définition juridique unique »
- « L'aspect international »
- « Les disparités législatives à l'échelle mondiale »

[19] www.internet-signalement.gouv.fr/

- « Le manque d'expertise technique des victimes individuelles ou par désir de préservation de la réputation des organisations »

À ce que nous éclairons jusqu'à présent, nous ajoutons « le désir de préservation de la réputation des organisations » (Côté, Bérubé et Dupont, 2016 : 206). En effet, il est dans l'intérêt des entreprises victimes de cyberattaques de ne pas dévoiler des intrusions ou toute autre cyberattaque. Ces données chiffrées constituent une absence qu'il est significative de noter.

Les cadres de référence des enquêtes statistiques privées ne sont pas tout à fait définissables, des cas particuliers surviennent comme le manque de sensibilisation de certains individus qui produisent une défaillance informatique involontaire (défaillance alors catégorisée comme une cyberattaque) et le détournement d'usage de logiciels qui ne sont pas malveillants à l'origine (Côté, Bérubé et Dupont, 2016 : 215). Ils expliquent que des « menaces jugées marginales ou non commercialement rentables » sont volontairement sous-évaluées car elles ne représentent pas un bénéfice selon les critères de l'entreprise émettrice du rapport. Les chiffres et typologies du cybercrime sont utilisés de manière très malléable suivant des besoins.

En outre, les complications de quantification du cybercrime sont aussi dues à des collectes de données excessivement variées et disparates. Les institutions étatiques, les organisations privées et les médias souhaitent tous rassembler des chiffres à ce sujet. « Il semble y avoir un décalage marqué entre la croyance envers la fiabilité des statistiques et l'utilisation déterminée par d'autres intérêts » (Côté, Bérubé et Dupont, 2016 : 209). Cette pluralité de sources n'est pas asymptomatique car elle génère de la désinformation. De surcroît, les trois scientifiques décrivent que cette croyance absolue envers les statistiques stimule leur prolifération. Les chiffres occupent une place importante en cybercriminalité puisqu'ils ont été au centre des études criminologiques passées (Côté, Bérubé et Dupont, 2016 : 207). Au sujet des enquêtes de victimisation publique, les auteurs tiennent à prendre du recul et se questionnent sur les défaillances potentielles engendrées par une base de données conçue sur le principe du volontariat des victimes qui osent en parler. Par ailleurs, il faut aussi tendre à se détacher des sources officielles qui ne sont pas représentatives à raison qu'une partie minoritaire est inculpée en matière de délits cybercriminels.

Les complications identifiées par les chercheurs obstruent une quantification efficiente de la cybercriminalité. L'absence de chiffres formels et l'impossibilité de mesurer le phénomène

engendrent de l'imaginaire et des représentations. À défaut de repères fondés, des acteurs non certifiés dans cette tâche de mesure s'adonnent aux discours en tout genre.

1.3. La construction d'une figure

La notion de représentation dans ce travail se doit d'être éclairée. Nous partons de la notion telle qu'Émile Durkheim la définie dans son raisonnement sociologique en 1898 au travers de trois réalités et spécifiquement des « représentations collectives » : c'est ce que nous retenons sous le terme de représentation du cybercriminel. Les représentations collectives incluent le mythe, la religion, … Elles sont une « réalité intériorisée », « une interprétation du monde physique et du monde social » (Danic, 2006 : 29). Pour autant, un aspect de la représentation du cybercriminel au sein de cette recherche se rattache également à la « représentation sociale » de Serge Moscovici sous l'angle de la psychologie sociale : la représentation sociale du cybercriminel se construit par une action, celle de réalisateurs qui sont la société et qui conceptualisent le cybercriminel. Sur une approche constructiviste, nous fixons la représentation du cybercriminel comme une réalité historique, la présence indéniable du cybercriminel aujourd'hui qui est construite par tous aux termes de relations sociales quotidiennes.

1.3.1. Schémas de pensées et producteurs de discours

L'évènement significatif qui va introduire Internet dans le débat public et l'opinion, créant des représentations et des schémas de pensées, est l'entrée du discours sur Internet au sein des médias traditionnels. Patrice Flichy inscrit cette période dans les années 1992-1993 avec ce qu'il nomme les « grands médias ». Il explique qu'une part de « l'utopie » provient des concepteurs eux-mêmes : « l'imaginaire proposé aux utilisateurs s'inspire largement des utopies de concepteurs mais qu'il a néanmoins subi un certain nombre de transformations » (Flichy, 2001 : 114). Cette phase où les concepteurs inspirent l'imaginaire est menée conjointement à leurs interventions discursives qui démocratisent l'outil dans le but d'aider à sa diffusion (Flichy, 2001 : 116). Avec les communautés virtuelles, la vulgarisation d'Internet par les prises de parole des informaticiens dans des ouvrages spécialisés (manuels, guides, …), des revues pour le grand public ou des magazines dédiés spécialement à Internet (« cyberrevue » comme *Wired*) pousse plus loin l'utopie, « le mythe d'Internet » (Flichy, 2001). Patrice Flichy parle de « cyberélite » pour qualifier ces individus (acteurs d'Internet dès son lancement, informaticiens chevronnés, …) qui vont s'engager dans la diffusion d'Internet par

le discours mystifié ; ces personnes devenant parfois même directeurs de publication pour un média ou leur propre média directement. La « cyberélite » dirige les « cyberrevues ».

De manière similaire à ce qui sera énoncé plus tard dans ce travail avec l'affaire de la disquette Sida par Antonio Casilli pour le cas des *hackers* et le travail de Patrice Flichy, les médias construisent une sémantique qui favorise l'imaginaire d'Internet dans son ensemble bien que certaines figures sont plus ciblées et propices à cela. Antonio Casilli s'emprunte à déconstruire trois représentations sociales répandues, trois idées perçues : l'image du *geek*/informaticien solitaire (« les internautes forcenés n'ont pas de relations sociales »), « Internet, territoire de la jeunesse » et « Internet est un monde à part déconnecté du réel » (Casilli, 2011).

Il commence par la représentation du *geek*/informaticien solitaire en démontrant que cette figure n'est qu'une image bien lointaine de la réalité des faits. Cette représentation est d'ailleurs reprise pour le cybercriminel dans l'imaginaire collectif. Antonio Casilli nous décrit cette représentation comme un phénomène qui n'est pas une nouveauté car ce stéréotype est pour la première fois présent dans « un ouvrage de 1976, *Computer Power and Human Reason*, que Joseph Weizenbaum dressa le portrait de ce 'forcené de l'ordinateur', à la mise 'négligée' et à l'hygiène 'approximative'. Aujourd'hui encore, l'emmuré, le *no-life* qui pallie une solitude douloureuse en multipliant les contacts en ligne est un grand favori des romanciers populaires, des commentateurs et des analystes culturels en quête de raccourcis » (Casilli, 2011 : 1). Ce modèle qui s'est imposé au fil du temps est faux, les interactions informatiques ne remplacent pas les interactions réelles pour les internautes les plus actifs mais viennent compléter les interactions préexistantes (Casilli, 2011). Elles enrichissent le lien social, nous pouvons faire le rapprochement avec Internet comme extension de la démocratie selon le point de vue adopté par Dominique Cardon.

Dans un second temps, il s'emploie à prouver qu'Internet n'est pas uniquement « le territoire de la jeunesse » comme cela est souvent affirmé. Il est d'autant plus intéressant que les *hackers* et cybercriminels sont fréquemment incarnés par des individus jeunes au cinéma pour ce que nous observerons. Grâce à des statistiques et à d'autres travaux comme ceux d'Eszter Hargittai (chercheuse en communication à l'Université de Zurich), Antonio Casilli affirme que les individus qui sont nés avec Internet ne sont pas tous à l'aise avec les Technologies de l'Information et de la Communication. Cependant, les « digital natives » remplissent d'autres besoins que les individus plus âgés qui ne sont pas nés à l'ère d'Internet n'éprouvent pas. Tout est une question de besoins et non de critères démographiques sur ces questions.

Pour terminer ses recherches, il démontre qu'Internet n'est pas un monde à part, monde qui n'a de raison d'être qu'en dehors de la société réelle. La sémantique d'Internet a construit son imaginaire, sémantique que l'on retrouve dans les magazines comme l'exemple qu'il nous donne avec la revue canadienne *Adbusters*. Nous rejoignons les propos de Patrice Flichy.

> *La sémantique d'Internet n'est pas avare de métaphores qui nous invitent à penser cet au-delà informatique comme, tour à tour, une mer sur laquelle 'naviguer' ou 'surfer', […]. Paradis utopique dans lequel régnerait l'harmonie sociale, cette représentation désincarnée du Web fait fi des conflits et mobilise à chaque pas des métaphores d'amour et d'amitié (les 'amis' et les 'j'aime' auxquels sont habitués les membres de Facebook).*
>
> *(Casilli, 2011 : 3)*

Après avoir cité l'œuvre *Neuromancien* (1984) de William Gibson pour expliciter l'évolution des représentations d'Internet, il conclut par des termes qui poussent les Sciences sociales à davantage s'intéresser aux détournements d'Internet, ce qui dans le cadre de ce présent TER, nous ouvre le champ de la cybercriminalité : « Les systèmes techniques ne peuvent pas être pensés en dehors des détournements auxquels leurs usagers les soumettront : c'est la justement le défi qui attend les sciences sociales dans les prochaines années » (Casilli, 2011 : 4).

Dans un autre axe de réflexion, les professionnels ainsi que d'autres personnalités médiatiques (consultants, journalistes spécialisés, …) entretiennent l'insécurité numérique ce qui est un facteur de production d'idéologie et d'imaginaire d'Internet. La culture de l'insécurité, entre réalité des risques et fantasmes au service de la représentation est le point de vue défendu par Benoît Dupont et Vincent Gautrais. Ils ciblent principalement les entreprises de sécurité informatique, entreprises fournissant des solutions réseau et/ou des anti-virus comme principales responsables de cet imaginaire. Benoît Dupont et Vincent Gautrais tirent ces conclusions en s'appuyant sur les rapports de sécurité et les études statistiques produites par ces entreprises (nous pouvons entre autre citer McAfee, Symantec, …) (Dupont et Gautrais, 2010). Ils soutiennent que les professionnels du secteur adoptent volontairement un discours « alarmiste » avec des éléments de langages exagérés pour servir des finalités économiques en leur faveur. Discours et encore une fois sémantique (*cf.* travaux de Patrice Flichy, Antonio Casilli, …) qui ne manquent pas d'être partagés par les « médias de masse » bénéficiant ainsi d'une portée bien supérieure à des travaux scientifiques plus fondés. De plus, les deux auteurs ajoutent que ses études privées reposent sur des protocoles flous où il est complexe de savoir

dans quelles conditions est menée la collecte de données. « Il importe de tenter de mesurer l'insécurité réelle ou présumée qui est associé à ce domaine tout neuf et qui ne manque pas de générer de nombreux fantasmes » (Dupont et Gautrais, 2010 : 1). C'est la représentation du *hacker* et du cybercriminel qui se trouve directement alimentée par ce type de contenus provenant du monde professionnel, la connaissance portant sur le champ d'action du cybercriminel est altérée.

Les internautes et les entreprises, eux-mêmes, nourrissent l'imaginaire d'Internet en entretenant des ambivalences. « L'utilisateur, […], va formuler en matière de cybersécurité des attentes et exigences diverses voire contradictoires. Car il veut à la fois circuler librement mais que l'on puisse piéger les internautes indélicats ou pédophiles. Que son commerçant en ligne comptabilise sa fidélité afin de lui offrir des tarifs préférentiels tout en étant attentif à la confidentialité de ses achats » (Arpagian, 2018 : 95). Ce schéma de pensées soulevé par Nicolas Arpagian floute les frontières de lutte en matière de cybercriminalité (les données relatives à des actes cybercriminels sont rares ou difficiles d'accès, nous avons développé davantage ce point précédemment) ce qui a pour symptôme d'encourager la représentation du cybercriminel. Le cybercriminel reste avant tout un internaute qui use ou détourne les outils numériques, mais ces choix paradoxaux provenant des internautes sur la confidentialité des données contribuent à le classifier comme un acteur à part. Le manque de connaissances au sujet de cette figure est porteur de fictions. De plus, les entreprises s'exposent à des risques cybercriminels qu'elles peuvent souvent éviter. L'ampleur des risques pris est mal calculée ce qui créé de nouvelles opportunités cybercriminelles ne pouvant être clairement délimitées. Nicolas Arpagian donne l'exemple des entreprises qui souhaitent bénéficier des technologies numériques mais qui externalisent leurs outils (smartphones pour les employés, sites internet, …) vers des infrastructures chez qui elles ne disposent pas d'une grande maîtrise, d'un contrôle suffisant (Arpagian, 2018 : 85). En optant pour ce type de prérogative, le champ d'action du cybercriminel s'élargit. La carence des entreprises sur ses questions et l'ajout de risques pourtant évitables brouillent l'information quant aux possibilités techniques qui s'avèrent disponibles pour le cybercriminel.

Le rapport de force inégalitaire entre « surveillants » et « surveillés » est aussi promoteur d'un discours autour d'Internet, Solange Ghernaouti et Arnaud Dufour nous font remarquer cette inégalité accompagnée de sources (Ghernaouti et Dufour, 2017 : 113). Pour illustrer ce propos, nous pouvons penser aux réseaux sociaux et aux politiques de confidentialité qui ne sont pas

toujours évidentes pour l'utilisateur mais pas uniquement. Les applications mobiles qui proposent un service de guidage routier grâce aux technologies de positionnement par satellites (GPS, …) sont d'importants collecteurs de données personnelles, celles-ci ne sont souvent pas connues de l'utilisateur. « La surveillance informatisée à très grande échelle se généralise et met en danger les libertés d'expression, d'association, d'information, […] » (Ghernaouti et Dufour, 2017 : 114). Cette liberté d'information est pourtant essentielle car le rapport de force inégalitaire qui s'exerce la diminue grandement. Les internautes savent que leurs données sont collectées en échange de services mais n'en connaissent que rarement plus. La désinformation est alors possible et laisse le champ libre à différents discours quant au niveau de l'intrusion dans la vie privée réalisable. Le Règlement Général sur la Protection des Données (RGPD) émis par l'Union européenne en 2016 tente de rectifier cette problématique. Nous pouvons également nous permettre de faire le lien avec la « présupposition d'égalité » (Cardon, 2010 : 79).

Pour désigner les acteurs qui produisent un discours inquiétant sur le cyberespace et ses dérives comme nous l'avons vu au fil des recherches menées, Benoît Dupont et Vincent Gautrais établissent un lien avec les recherches d'Howard Becker datées de 1985. Ces acteurs sont qualifiables « d'entrepreneurs de la morale » (Dupont et Gautrais, 2010 : 18). Simultanément aux paroles alarmistes, dans une toute autre optique, des discours de prévention sont mis au point par les instances officielles régulatrices du cyberespace dans le but d'assurer un terrain de moins en moins propice à la cybercriminalité (Ghernaouti et Dufour, 2017). De même, ces discours de prévention sont aussi diffusés et adaptés par les professionnels. Il convient de réfléchir à l'exagération ainsi qu'aux formulations employées pour communiquer à ce sujet.

Figure 2 : image tirée du rapport annuel de Norton par Symantec et « Survival Guide » (Source : LaPresse.ca et Norton.com)

Patrice Flichy distingue les concepteurs (chercheurs du MIT et d'autres laboratoires, Nicholas Negroponte, Douglas Carl Engelbart, …) et les promoteurs (Howard Rheingold, …) en tant qu'acteurs qui médiatisent Internet. Un cheminement entre ses deux partis est porteur de sens. Avec les communautés virtuelles, il souligne un « imaginaire de masse » ainsi qu'une « aura » (Flichy, 2001 : 116). Les termes choisis témoignent d'une réception à l'échelle sociétale.

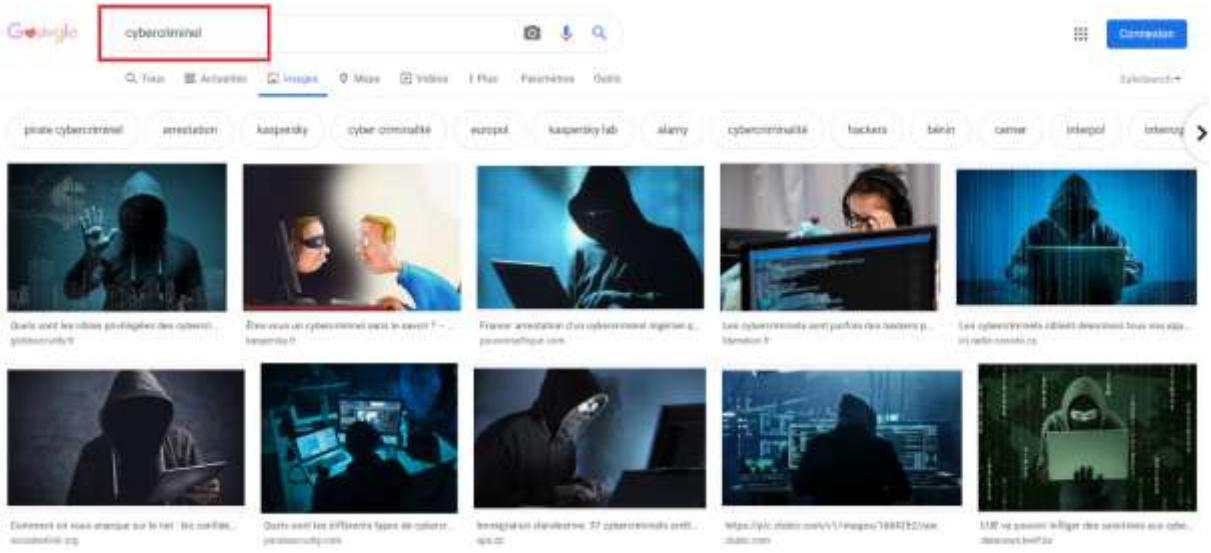


Figure 3 : résultats de recherche pour le mot clé « cybercriminel » depuis Google Images, en navigation privée au 14/02/2020 (Source : Google Images)

Sur Internet, on retrouve toujours cette figure assise dans l'ombre, devant son ordinateur, qui semble écrire des lignes de code d'une grande complexité ; en témoigne le code informatique qui chute en arrière-plan. Le regard est mystérieux parfois indiscernable. Cette représentation du cybercriminel occupe une place importante alors qu'elle est pourtant disjointe de la réalité. Elle se trouve complètement mystifiée. La représentation du cybercriminel est nourrie par la figure du criminel traditionnel (voleur, malfaiteur, …) car elles ont toutes deux des similarités essentielles : points communs visuels comme la cagoule, objet symbolique de l'anonymat et du criminel en complément de points communs méthodologiques comme nous l'avons vu (motivations, opportunités, …).

Nous reconnaissons ici tout ce que Roland Barthes a défini en tant que mythe (Barthes, 1957 : 211). La représentation du cybercriminel véhicule un message qui n'est pas exempt de signes. Les signes se manifestent dans l'apparence physique prononcée qui est prêtée au cybercriminel. Le cybercriminel incarne la peur de l'internaute qui souhaite préserver sa vie privée, il incarne le vol des données, l'intrusion dans l'intimité. Il est le mal du cyberespace. Sa représentation atteste de ses compétences étendues et méconnues de tous, son action se résumant à une

imposante quantité de données très codifiées. Le cybercriminel est emprunt à un « usage social qui s'ajoute à sa pure matière » (Barthes, 1957 : 212). Si le cybercriminel est perçu de cette manière c'est parce qu'il y a eu une appropriation sociale du terme qui suscite une représentation.

Figure 4 : stéréotype, représentation du cybercriminel (Source : Google Images)

1.3.2. La représentation dans les médias et les œuvres culturelles

Jusqu'alors bien méconnus en dehors des universités et du monde assez fermés des passionnés de programmation, c'est au début des années 1980 que les premiers *hackers* vont se voir progressivement médiatisés grâce aux œuvres culturelles qui font parler d'elles. Le film le plus emblématique à ce moment est *WarGames* qui sort en 1983. Fréderic-Jérôme Pansier et Emmanuel Jez le décrivent comme « exagérant volontairement les possibilités techniques des appareils de l'époque, cette fiction eut pour principal vertu de révéler l'existence des *hackers*, une catégorie d'individus hautement qualifiée en techniques informatiques et fascinée par le cyberespace et son côté ludique. Mesurer leurs capacités techniques en s'introduisant dans des systèmes informatiques complexes leur apparait un jeu de l'esprit » (Pansier et Jez, 2000 : 99). Le film reçoit un accueil retentissant à sa sortie et se voit nommé aux Oscars. Le principal protagoniste, un jeune pirate informatique inscrit alors la première représentation du *hacker* dans l'espace public : un individu jeune, très doué, qui s'infiltre involontairement dans un réseau informatique hautement sécurisé appartenant à une institution étatique. Portrait se rapportant déjà à un acte frauduleux bien qu'involontaire, les frontières entre ce que nous qualifions aujourd'hui d'acte cybercriminel et la représentation sociale des *hackers* sont particulièrement poreuses. De plus, les *hackers* ne revendiquent pas ouvertement la compétence de s'introduire dans des systèmes informatiques bien qu'une partie d'entre eux bénéficient de cette compétence. Conjointement à l'idée d'individus surdoués techniquement évoquée par Fréderic-Jérôme Pansier ainsi qu'Emmanuel Jez pour décrire la représentation des *hackers* dans le film *WarGames,* Thierry Paquot se penche sur l'impact du cinéma en matière de production de stéréotypes qui sont des exagérations de certains traits propres à un individu dans la société.

« Le cinématographe, dès sa naissance en 1895, va fabriquer des « stéréotypes » […] » (Paquot, 2019 : 120). Il montre avec le stéréotype du « patron » en exemple, la faculté du cinéma à retranscrire la représentation qu'une société se fait d'un individu, d'une figure, d'un statut. Le cinéma est un reflet des schémas de pensées de la société, les représentations et stéréotypes évoluant à son rythme.

Dans son travail sur l'affaire de la disquette Sida, affaire très populaire en 1989 qui dévoile l'utilisation d'un rançongiciel (*ransomware*)[20] dans une disquette à but pédagogique, Antonio Casilli démontre l'impact des médias et plus précisément le rôle de la presse dans la construction de l'image des *hackers* en tant que cybercriminels. Il utilise pour cela un corpus d'articles de presse.

> *Avant 1988, les métaphores les plus communément empruntés sont de nature militaires : les hackers 'attaquent' (attack) et 'envahissent' (invade) les systèmes informatiques des entreprises pour les 'espionner' (spy) […]. Aussi les médias privilégient des histoires dans lesquels les malfaiteurs sont des jeunes adeptes de 'jeux de guerre' (wargames) et les victimes, typiquement, des agences militaires et de sécurité nationale*
>
> *(Casilli, 2015 : 3)*

Le film *WarGames* en est un bon exemple également. En outre, cette recherche prouve l'importance qu'occupent la sémantique et les médias dans la construction d'une image et d'un discours qui est dans le cas présent, celui sur les *hackers*. Cette affaire emblématique marque le tournant du passage d'une sémantique militaire à une sémantique de la viralité selon Antonio Casilli d'où les termes de « virus », « infection » que l'on trouve plus communément pour désigner certains concepts informatiques. Le *hacker* acquiert au fil des années une image péjorative qui est celle du criminel auprès du grand public. Antonio Casilli définit le Dr Popp (responsable de l'élaboration et de la diffusion de la disquette Sida dans l'affaire) comme « un 'cybercriminel' dans l'air du temps » et mentionne le rapprochement de ses actes avec l'éthique *hacker* que nous avons développé précédemment. Encore une fois, on remarque que la frontière entre cybercriminel et *hacker* est floue, les médias rendant cette distinction de plus en plus complexe.

[20] *cf.* Glossaire

De manière additionnelle, la démocratisation d'Internet à partir des années 1990 participe aussi à ce changement. En effet, les *hackers* sont les premiers actifs lorsqu'Internet apparaît, seulement, avec l'arrivée de l'ordinateur portable et l'accès généralisé à l'informatique de bureau, vient le grand public, les grandes entreprises et les organisations étatiques. Ces autres acteurs, issus du monde réel, intègrent l'utilisation de cette nouvelle technologie et souhaitent prendre le contrôle sur ce nouveau terrain : les grandes entreprises ont pour principaux objectifs d'étendre leur dimension commerciale et les organisations étatiques quant à elles souhaitent légiférer le Web. C'est en ce sens que les principes de netiquette verront notamment le jour, véritables compromis entre éthique des internautes de la première heure et lois régissant le « monde réel ». Dès cet instant, les *hackers* deviennent une minorité d'internautes sur le Web et l'esprit originel du *hacking* est peu à peu oublié. « Les *hackers* de la technologie informatique considère que l'âge d'or s'achève avec l'expérience de la répression policière et judiciaire » (Dagiral, 2008 : 488). Les *hackers* se réunissent davantage dans des groupes dédiés avant de devenir les principales cibles pour tout ce que le grand public rencontre de mauvais sur ce nouvel outil qu'est Internet : virus, piratage, vol de données, … Les hackers sont les responsables.

> *Ce moment correspond à la construction d'une représentation sociale négative des hackers, qui deviennent des pirates au sens où cela est toujours communément entendu aujourd'hui : par leur faute, la sécurité devient une préoccupation majeure des acteurs de l'informatique et de ses réseaux, et l'analogie hackers et terroristes devient un lieu commun*
>
> *(Dagiral, 2008 : 488)*

Si les médias, suivant le nombre exponentiel de machines connectés au réseau des réseaux, ont tenu un rôle primordial dans la modification de la représentation des *hackers* auprès du grand public, d'autres acteurs sont à prendre en compte. En effet, n'importe quel internaute peut se revendiquer *hacker* ce qui va poser problème. Certains individus qui s'introduisent dans les systèmes informatiques, qui créent des logiciels malveillants ou encore qui s'adonnent à du sabotage de matériel informatique vont se revendiquer en tant que tel. Des statuts émergent en fonction des pratiques auxquelles chaque individu participe, avec pour les plus connus :

- *black hat* (signifiant ceux qui s'adonnent à des pratiques illégales comme les intrusions dans les systèmes mais également ceux qualifiés de *crackers* qui piratent les logiciels) ;

- *white hat* pour les *hackers* au sens traditionnel comme nous l'avons vu ;
- *grey hat* pour des individus aux actions plus nuancées, oscillant entre *white hat* et *black hat.*

Éric Dagiral parle de « lutte du Bien et du Mal » et d'une « lutte pour la reconnaissance » de manière plus globale pour catégoriser cette situation (Dagiral, 2008 : 490). Nous pouvons constater l'étendue de ce qui est finalement sous-entendu sous le terme *hacker* qui évolue dans le temps.

La complexité est qu'en un sens, les cybercriminels sont qu'une sous-catégorie de *hackers* aujourd'hui (*les black hats*) et dans un autre sens, ils ne sont pas des *hackers* pour les *white hats* ou *hackers* traditionnels. Certains *hackers* célèbres n'hésitent d'ailleurs pas à prendre la parole pour dénoncer la non-appartenance des *black hats* au mouvement des *hackers* et soutiennent les initiatives de netiquettes quand d'autres affichent un « esprit de méfiance vis-à-vis des lois de la société : John Berry Barlow[21] a ainsi proclamé l'indépendance du cyberespace dans une célèbre déclaration » (Dagiral, 2008 : 492). En outre, un autre paradoxe apparaît qui est celui que les *white hats*, bien que servant une cause éthiquement juste, usent de méthodes parfois illégales (pour une partie d'entre eux) selon la législation du gouvernement auquel ils appartiennent pour parvenir à leurs fins bienveillantes. Éric Dagiral soulève aussi une ambivalence supplémentaire autour des *black hats* : « parmi les pirates désignés sous le nom de 'crackers' se trouvent des personnes désireuses de rendre accessibles à tous, gratuitement ou quasi gratuitement, produits culturels et logiciels nécessaires à l'activité créative. Le contournement des mesures de protections s'inscrit dans une entreprise non lucrative orientée vers la circulation des programmes, se réclamant de la liberté d'accès à l'information » (Dagiral, 2008 : 493). Nous retrouvons ici l'emprunt des principes de l'éthique *hacker* mais aussi une certaine idéologie de la contre-culture américaine des années 1960.

Il y a donc de réelles questions qui restent encore sans réponses pour qualifier certains *hackers*, tous les *hackers* ou des internautes extérieurs de cybercriminels. Bilel Benbouzid et Daniel Ventre, en mentionnant la faible quantité de travaux en Sciences sociales sur le crime en ligne, parlent de « *hackers* malveillants » et évoquent « la résistance du sociologue à envisager le *hacking* comme un problème criminel, voire même une question de déviances. L'objet '*hacker*' se laisse difficilement saisir par une sociologie du crime, d'où le faible volume de recherches

[21] https://fr.wikipedia.org/wiki/John_Perry_Barlow

en France » (Benbouzid et Ventre, 2016 : 13). Dans une seconde optique, les deux chercheurs mettent en avant une sociologie du crime en ligne qui exploite la figure du *hacker* comme une menace et à la fois une ressource avec l'appui de travaux menés par d'autres chercheurs français : « À la fois menace et ressource, les *hackers* tissent des liaisons dangereuses avec les entreprises d'informatique et les éditeurs de logiciels en sécurité » (Benbouzid et Ventre, 2016 : 14). Ils exposent succinctement le profil de l'expert informatique qui mène une double vie en travaillant pour une entreprise informatique, voire de sécurité informatique directement et qui est simultanément membre d'une communauté de *hackers*. Configuration qui s'est démontrée par des cas biens réels. Enfin, ils énoncent une caractéristique similaire à toutes les recherches qu'ils examinent : « […] le point commun à toutes les trajectoires analysées est le fait que le *hacker* est vulnérable à des sollicitations douteuses qui sont propres aux dynamiques de la 'professionnalisation' dans le champ de l'informatique » (Benbouzid et Ventre, 2016 : 15).

En se diversifiant, les *hackers* font apparaître de nouvelles ramifications symbolisant leurs activités dont le néologisme de forme *cyberhacktivisme,* aussi nommé par cybermilitantisme, qui manifeste une prise de position (politique, religieuse, …) au moyen de l'informatique et du piratage. L'idée est de faire passer un message grâce à des canaux technologiques. Solange Ghernaouti et Arnaud Dufour rédigent la définition suivante : « Le *hacktivisme* ou *cyberactivisme* est une forme de protestation basée sur l'usage des outils digitaux et de cyberattaques pour promouvoir des idéologies ou des objectifs particuliers » (Ghernaouti et Dufour, 2017 : 105). Il est pertinent de remarquer que les « cyberattaques » font pleinement parti de ce type d'action ce qui est une forme de cybercriminalité. Nous notons d'ailleurs que cette définition englobe le terrorisme à l'ère numérique puisqu'elle évoque la promotion d'une idéologie. De surcroît, ce passage se situe dans une partie intitulée « Cyberactivisme et cyberterrorisme » issue du chapitre « Cybercriminalité et cybersécurité » au sein de l'ouvrage (Ghernaouti et Dufour, 2017). Le *hacker* est considéré en cybercriminel. L'Histoire n'est pas en manque d'exemples pour ce qui relève du cybermilitantisme ; le groupe d'*hacktivistes* Anonymous est l'un des plus connus à ce jour pour avoir revendiqué de nombreuses attaques à travers le monde dont certaines attaques récentes en soutien au mouvement des « Gilets Jaunes » apparu en France durant l'année 2018.[22] Sous un autre angle, le célèbre *hacker* australien Julien Assange est connu pour avoir révélé de nombreux scandales depuis son

[22] https://www.lemonde.fr/pixels/article/2018/12/13/gilets-jaunes-la-dgsi-enquete-sur-des-attaques-informatiques-et-des-fuites-revendiquees-par-des-anonymous_5397053_4408996.html

organisation Wikileaks qu'il fonde en 2016 avec des sources et des moyens d'obtention de l'information qui restent bien méconnus.

Dans un billet de recherche publié en mars 2020, plusieurs chercheurs français font état « d'une bipolarisation manichéenne » du *hacker* par les médias audiovisuels français et précisément par les contenus provenant des journaux télévisés (Bertin et al., 2020). Ils mettent en évidence une évolution de la figure du *hacker*.

1.3.3. Le mouvement cyberpunk

Le mouvement cyberpunk apparaît au début des années 1980 accompagnant les avancés de l'informatique et d'Internet. Reprenant les codes de la contre-culture américaine des années 1960, ce mouvement a pour principale nouveauté l'ajout de la technologie à des thématiques déjà existantes comme le mouvement « punk » tel que son nom l'indique. Ce courant naît de la rencontre entre la figure du *geek* et *hacker* avec la musique rock, l'idéologie libertaire et d'autres principes de la contre-culture. Il est largement popularisé par deux romanciers américains de science-fiction que sont Bruce Sterling et William Gibson qui créent un univers fictionnel autour du mouvement. En effet, tous deux écrivent des ouvrages littéraires qui sont accueillis avec succès lors de leur parution comme *Neuromancien* (1984) pour William Gibson ou la série de nouvelles *Mozart en verres miroir* (1986) pour Bruce Sterling. En plus de fonder le mouvement cyberpunk, ses ouvrages participent à la création du style littéraire cyberpunk, véritable branche de la science-fiction, qui est par la suite repris dans des œuvres d'autres domaines culturels (cinéma, photographie, architecture, jeu, …). Si le mouvement cyberpunk prend une place importante dans la représentation du cybercriminel, c'est parce que celui-ci a fortement contribué à nourrir cette figure numérique en la présentant dans diverses histoires. Ce courant met souvent en scène un *hacker* ou un cybercriminel solitaire qui se refuse à être aliéné par la société, dans un monde proche du *post*-apocalyptique. Le personnage fait face à de grandes entreprises qui prennent possession des technologies dans un objectif non éthique. Le monde est sombre et ne s'annonce guère meilleur. « Les influences culturelles du *hacking* sont principalement dictées par la ligne idéologique propre au mouvement littéraire et philosophique du cyberpunk. […] le cyberpunk naît de la peur du *Big Brother*[23]. Il met en avant un comportement subversif […] » (Pansier et Jez, 2000 : 101). Nicolas Arpagian résume l'œuvre *Neuromacien* (1984) de William Gibson par les mots suivants : « […] trilogie qui a

[23] Expression inventée et popularisée par Georges Orwell en 1984, elle désigne aujourd'hui les abus de pouvoirs et les atteintes à la vie privée.

pour personnage central un voleur de données. Celui-ci est en mesure d'établir des connexions entre son esprit et un réseau mondial reliant entre eux des ordinateurs » (Arpagian, 2018 : 9).

Etymologiquement, Nicolas Arpagian nous rappelle l'origine du mot qui est la contraction du terme « cybernétique » avec le terme « punk ». « La création du mot 'cybernétique' revient à un professeur du *Massachusetts Institute of Technology* (*MIT*), Norbert Wiener, qui, dans un ouvrage de 1948[24], désigna par ce vocable le 'champ entier de la théorie de la commande et de la communication, tant dans la machine que dans l'animal' » (Arpagian, 2018 : 9). En outre, il justifie la démocratisation du préfixe « cyber » dans l'environnement sémantique qui encadre aujourd'hui Internet (cybercriminalité, cybersécurité, cybermilitantisme, …) grâce au premier emploi du terme « cyberespace » par William Gibson dans *Neuromancien* (1984). Pour Stéphane Leman-Langlois, l'utilisation de ce qu'il nomme les « cybermots » provient de cette même origine à laquelle la cybercriminalité renvoie également (Leman-Langlois, 2006 : 65). Il définit plus en détails le cyberspace afin de clarifier son usage encore hasardeux : « le cyberespace s'oppose à l'espace conventionnel au sens où il est affranchi de toute localisation physique ou géographique. Ce n'est pas un endroit mais un point de rencontre de flux informationnels portés par des réseaux interconnectés. […] Il existe une certaine parenté entre ce cyberespace et l'espace culturel où ont toujours été construites les notions de criminalité, de criminel, de droit, de responsabilité, de bien, de mal, etc. » (Leman-Langlois, 2006 : 66).

Le mouvement cyberpunk nous renseigne sur les représentations du cybercriminel mais également sur l'origine des termes que le débat publique et les médias emploient aujourd'hui sans forcément davantage de précisions. Il nous permet de replacer les mots dans leur contexte d'origine.

Dans cette grande première partie, nous avons étudié le passage du *hacker* aux cybercriminels en déconstruisant les imaginaires. Nous avons convoqué les auteurs de champs scientifiques complémentaires pour bien saisir la construction de la représentation du cybercriminel. En un premier temps, nous sommes passées par les origines d'Internet car elles ont suivies et façonnées la cybercriminalité et sa représentation. Par la suite, nous avons également abordé l'acte cybercriminel et la cybercriminalité grâce aux travaux scientifiques existants pour comprendre ce qui les caractérisaient. Nous avons rendu compte de la complexité du terme « cybercriminel » et de ses raisons tout en la confrontant à la science. Enfin, nous nous sommes

[24] Wiener, N. (1948). Cybernetics. Paris, France : Hermann.

focalisés sur la construction de la figure du cybercriminel en nous penchant sur les acteurs du discours, les schémas de pensées existants, le cybercriminel tel qu'il est dépeint dans les médias et les œuvres culturelles pour conclure par l'influence du mouvement cyberpunk.

2. Caractériser les représentations

Avant de présenter en détails le protocole de recherche, il est nécessaire de préciser certains points et plus particulièrement notre posture épistémologique. Dans le cadre de ce travail, nous sommes dans une observation de représentations sociales pour tenter de répondre à notre problématique : quelle est la représentation du cybercriminel aujourd'hui ? De cette problématique découle deux sous-questions : comment s'est construite cette représentation à travers les œuvres culturelles ? Quelle en est la portée sur le terrain professionnel ?

Notre posture sociologique vise à comprendre les représentations au travers des comportements des personnages décrits dans le corpus. Nous nous attachons ainsi aux significations et aux processus sociaux à travers les œuvres culturelles. Les démarches d'observation et de restitution mobilisées sont étiques, nous nous posons en observateur en nous fixant sur des faits visibles par tous (les œuvres culturelles) ; par l'utilisation systématique d'un tableau, nous prenons néanmoins en ligne de compte la dimension subjective qui peut apparaître. Nous faisons également le choix d'une posture qualitative au sein de ce protocole de recherche, nous justifions ces choix dans la partie suivante dans le but de mieux en assurer la compréhension une fois dans le contexte.

2.1. Présentation du cadre méthodologique

Pour comprendre la représentation du cybercriminel aujourd'hui et observer sa construction au fil des années, nous faisons le choix de nous tourner vers un corpus d'œuvres culturelles à analyser. Ces œuvres culturelles sont majoritairement cinématographiques, celles-ci constituent un vecteur d'information important au sujet des représentations car elles sont imagées par les réalisateurs eux-mêmes et en cela incarnées dans un visuel quand une œuvre littéraire laisse une plus grande place à l'imaginaire. Comme nous l'avons vu dans les parties qui précèdent, le cinéma n'est pas avare de représentations en tout genre et participe pleinement à la construction de stéréotypes, la mondialisation jouant son rôle de diffusion.

Nous avons donc collectés 70 œuvres (cinématographiques, télévisuelles et vidéoludiques) allant de 1982 jusqu'à 2019. Les années 1980 sont la période où les premiers films évoquant l'informatique, Internet et les cybercriminels font leur apparition. Par conséquent, l'analyse des œuvres est diachronique.

Période chronologique de l'œuvre	Nombre d'œuvres culturelles analysées
[1982-1990]	3
]1990-2000]	13
]2000-2010]	20
]2010-2019]	34
Total	70

Tableau 3 : nombre d'œuvres culturelles analysées par période chronologique

2.1.1. Sélection et collecte des œuvres

Dans la phase de recherche, les œuvres ont été trouvées par différents biais. Les premières œuvres sont celles que nous avons récolté par l'intermédiaire des pages de résultats enrichies du moteur de recherche *Google*. En effet, *Google* met en place une liste de films jugés pertinents en fonction des mots clés entrés en guise de requête. Pour cela, nous avons effectué des recherches avec les mots-clés suivants : « films sur les cybercriminels », « films sur le cybercrime », « films sur les hackers », « films sur les informaticiens », « films sur internet », « films sur les pirates informatiques ». [25]

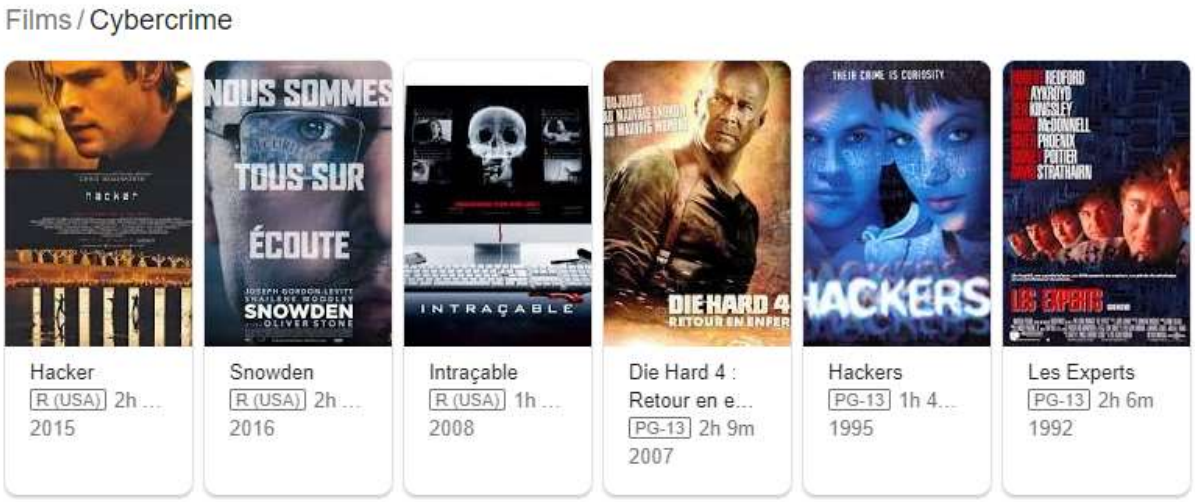


Figure 5 : résultats d'une requête Google pour la recherche « films sur les hackers » (Source : Google)

En un second temps, trois autres sources se sont avérées bénéfiques pour collecter des œuvres spécifiquement cinématographiques et télévisuelles sur la cybercriminalité : les sites spécialisés

[25] Ces mêmes requêtes ont été également formulées en anglais pour les films, les œuvres vidéoludiques et les contenus télévisuels.

sur l'audiovisuel (*Allociné*[26], *Télérama*[27], *Première, ...*), les sites d'actualité publiant des articles en lien avec le sujet (*Slate*[28], *Numerama*[29], …) et les sites proposant des classements de films qui portent sur cette thématique du cybercriminel. Pour cette troisième catégorie, c'est notamment le cas du site internet de l'entreprise *Kaspersky*[30] ou d'autres blogs dédiés. Les sites spécialisés sur le cinéma disposent de bases de données conséquentes, elles sont une ressource plus qu'utile à questionner et offrent la possibilité de trouver d'autres films selon plusieurs filtres de recherches intéressants (par type de film, par réalisateur, par thématique, …). Découvert au fil des recherches lors de la collecte des œuvres, le site internet *MovieCode*[31] a permis d'ajouter des œuvres à ce travail car celui-ci référence toutes les apparitions de code informatique au cinéma. Après des recherches plus approfondies dans un registre plus technique, le site Web du logiciel de cybersécurité *Nmap* (voir scanner de ports)[32] référence toutes ses apparitions dans les œuvres cinématographiques et télévisuelles, captures d'écrans étudiées à l'appui. Enfin, la plateforme *YouTube* a été une solution pertinente pour palier à la collecte d'œuvres car on y trouve une multitude de « *hacking scene* » (scène de piratage) permettant d'identifier les cybercriminels issus aussi bien de films et séries télévisuelles que des jeux vidéo avec des vidéos de *gameplay* riches en informations (cinématiques, …).

Au début des recherches, les œuvres littéraires (bandes dessinés, romans, …) évoquant un ou des cybercriminels devaient être présentes dans ce protocole. Seulement, il s'est avéré que la recherche d'informations précises en ligne sur ce type d'œuvre n'a pas porté ses fruits dû à un manque d'informations et/ou à un référencement insuffisant. Hormis de courts résumés, très peu des données recherchées sont disponibles. Par conséquent, nous avons donc recentré nos choix sur les œuvres cinématographiques, télévisuelles et vidéoludiques. Au fil des recherches, nous avons remarqué en outre un faible nombre d'œuvres vidéoludiques présentant explicitement le cybercriminel. En effet, à l'image de *Virus : The Ga*me (1997), *Uplink* (2001) ou encore de *868 - HACK* (2013), les jeux vidéo mettent davantage en scène l'acte cybercriminel en lui-même par la technique que le cybercriminel. Ceux-ci sont majoritairement construits autour du joueur qui interagit dans une interface informatique fictionnelle et attrayante, disjointe de la réalité. Toutefois, des œuvres vidéoludiques se démarquent de ce

[26] http://www.allocine.fr/article/fichearticle_gen_carticle=18640566.html
[27] https://www.premiere.fr/Cinema/Cinq-films-et-series-a-voir-avant-de-jouer-a-Watch-Dogs-2
[28] http://www.slate.fr/story/28737/social-network-internet-au-cinema
[29] https://www.numerama.com/tech/181512-de-tron-a-mr-robot-cinema-represente-monde-numerique.html
[30] https://www.kaspersky.fr/blog/top-10-des-films-sur-le-piratage/1490/
[31] https://moviecode.tumblr.com/
[32] *cf.* Glossaire

schéma et ont ainsi pleinement leur place dans ce protocole car elles mettent un accent plus prononcé sur la narration autour du cybercriminel. C'est notamment le cas de la série de jeux vidéo *Watch Dogs* (2014) où le joueur incarne le protagoniste Aiden Pearce qui est un cybercriminel. En tant que joueur, nous découvrons sa vie sociale, ses actions, son comportement dans un environnement en trois dimensions : des données précieuses pour ce travail de recherche.

Type d'œuvre	Nombre d'œuvres culturelles analysées
Films	57
Série TV	7
Jeu vidéo	6
Total	70

Tableau 4 : nombre d'œuvres culturelles analysées par type d'œuvre

2.1.2. Critères de la grille d'analyse

Les œuvres sont répertoriées de façon ordonnée dans une grille d'analyse en fonction de plusieurs critères que nous allons explicités (*cf.* Annexe 13).

Premièrement, les informations génériques des œuvres sont classées : nom, réalisateur(rice), date de sortie, genre, pays d'origine. Par ailleurs, les films sont répertoriés selon un numéro d'œuvre pour des questions de praticité. Ces critères basiques servent à identifier l'œuvre distinctement. Un critère spécifique a toutefois été ajouté à cette partie d'identification de la grille : l'accès à l'œuvre qui est soit complet ou partiel (C ou P dans la grille d'analyse). En effet, il est complexe de visionner toutes les œuvres du corpus et cela est une de ses limites principales dont nous avons pleinement conscience. Découlant de cette raison, les œuvres qui n'ont pas été visionné ou joué intégralement sont indiquées avec la donnée « P » pour Partiel afin de rester objectif durant l'intégralité du protocole de recherche comme le montre le Tableau 5.

N° d'œuvre	Type d'œuvre	Nom de l'œuvre	Accès complet/partiel (C/P)	Sexe du/de la réalisateur(trice) (H/F)	Date de sortie	Genre	Pays d'origine
1	Film	Tron	P	H	1982	Science-fiction	Américain

Tableau 5: données génériques de l'œuvre depuis la grille d'analyse

La collecte de données relatives à chaque œuvre à accès partiel se doit d'être développée pour plus de de compréhension. Afin de rendre possible cette collecte sans un accès complet à

l'œuvre, l'encyclopédie libre Wikipédia a été utilisé et plus particulièrement la version anglaise qui, en plus de contenir un accès à l'information plus complet sur certaines pages d'œuvre, se compose de la rubrique « *Plot* » proposant le scénario de l'œuvre en question. De plus, le visionnage des bandes annonces, des « *hacking scene* » d'œuvres en accès partiel apporte des données essentielles à la collecte étant donné que dans quelques œuvres, le cybercriminel ne fait que des apparitions succinctes ou partielles (Dennis Nedry avec son logiciel malveillant *Whte rbt.obj* dans *Jurassic Park* de 1993, Travis Dane dans *Piège à grande vites*se de 1995, Boris Grishenko dans *GoldenEye* de 1995, …). Les Wikis et autres *Fandom*[33] relatifs à une œuvre spécifique ont également été consulté. Ces sites internet communautaires sont tenus par des fans et regroupent des fiches personnages (contenant âge, profession, ...), des descriptions détaillées : ils offrent l'opportunité de trouver des informations précises sur une œuvre ou sur un détail présent dans l'œuvre. Lors de l'absence de séquences vidéo ou de textes dévoilant un cybercriminel dans certaines œuvres datées ou mal référencées sur ce point (Owen Reilly dans *Intraçable* de 2008, The Voice dans *Getaway* de 2013, …), *Google Images* est sollicité et permet d'identifier visuellement les cybercriminels concernés.

La seconde partie de la grille d'analyse, illustrée par le tableau 6, est celle qui nous intéresse le plus car elle se focalise directement sur notre objet d'étude : la représentation du cybercriminel.

Unique ou multiple (U/M)	Sexe (H/F)	Tranche d'âge	Profession	Lien de la profession avec le numérique	Groupe socioprofessionnel (PCS - 2003)
U	H	25-50	Programmeur	Liée au numérique	Professions intermédiaires

Acte(s) cybercriminel(s)	Lien social	Style vestimentaire/ apparence physique	Notes
Création d'un logiciel malveillant	Famille, virtuel et réel	Correct	Kevin Flynn : Il a développé CLU, une solution logicielle qui l'aide à solutionner illégalement ses problèmes de factures mais également à s'introduire dans les serveurs d'ENCOM pour chercher des lignes de codes spécifiques lui appartenant.

Tableau 6 : données relatives au cybercriminel représenté dans l'œuvre depuis la grille d'analyse

[33] *cf.* Glossaire

Cette seconde partie rassemble sous plusieurs aspects le cybercriminel principalement représenté dans l'œuvre. Le premier point porte sur la multiplicité ou non des individus cybercriminels au sein de l'œuvre (« Unique » ou « Multiple »). En effet, des œuvres mettent en scène plusieurs cybercriminels dans leur intrigue *(Die Hard 4 : Retour en enfer* de 2007, *Mr. Robot* de 2015, …), notre choix se tourne donc vers celui qui est le plus mis en valeur dans l'œuvre et par analogie celui dont l'œuvre nous donne le plus de données à récolter. Par la suite, nous classifions la tranche d'âge (0-15 ans, 15-25 ans, 25-50 ans, 50 ans et plus) du cybercriminel, sa profession et avec de manière plus formelle sa catégorie socioprofessionnelle selon la nomenclature établie par l'Insee (Utilisation du Niveau agrégé : 8 postes dont 6 pour les actifs[34]) dans le but d'harmoniser les données recueillies. Vient ensuite le(s) acte(s) cybercriminel(s) présent(s) dans l'œuvre. Pour cette catégorie spécifique, nous avons décidé de nous orienter sur le parti pris de l'acte cybercriminel que proposent Bilel Benbouzid et Daniel Ventre et que nous avons vu précédemment comme un assemblage entre crime et Internet : « Peu importe le degré de spécificité de l'acte malveillant, le crime et Internet sont rassemblés dans une même problématique pour comprendre ce que l'un fait à l'autre et vice-versa » (Benbouzid et Ventre, 2016 : 11). Nous faisons le choix d'identifier toutes les pratiques malveillantes liants crimes et Internet en nous fixant également sur les termes spécifiques donnés par les chercheurs et les professionnels pour définir des actions cybercriminelles précises (*phishing*, *phreaking*, attaque par force brute, attaque par dictionnaire, *backdoor*, *carding*, ver informatique, ingénierie sociale, enregistreur de frappe, …)[35]. Conformément à ce qui est évoqué dans les travaux d'autres chercheurs, aucune définition scientifique stable n'est encore établie. Puis, nous qualifions les relations sociales entretenues par le cybercriminel représenté au travers de quatre possibilités : famille, virtuel, réel et aucun (plusieurs modalités sont bien évidemment envisageables simultanément). Pour trouver ses informations, nous analysons le cybercriminel dans l'œuvre et observons si celui-ci à des relations régulières avec ses amis, ses collègues de travail, sa famille, … Cela se traduit par l'observation des cinématiques dans le cas des contenus vidéoludiques, par les séquences concernées dans les œuvres cinématographiques et télévisuelles. En conclusion, le style vestimentaire, l'apparence physique du cybercriminel est évaluée sur trois choix : atypique, correct et soigné. L'objectif n'est absolument pas d'émettre un jugement ou de discriminer mais d'observer les différences qui peuvent s'opérer dans les représentations physiques, esthétiques du cybercriminel. Nous nous basons sur les signes linguistiques et spécifiquement le signifié. Concrètement, nous

[34] https://www.insee.fr/fr/statistiques/fichier/2400059/PCS%202003%20_%20Guide%20[2016-11-21].pdf
[35] *cf.* Glossaire

pouvons donner l'exemple de Lisbeth Salander (cybercriminelle dans la série cinématographique et littéraire *Millenium*) présente dans notre grille à qui nous avons attribué la donnée « Atypique ». En effet, il est peu commun que des enquêteurs (dans le cadre de sa profession) s'habillent de cette manière (proche du style gothique) pour venir sur leur lieu de travail. Dans un même registre, nous pouvons nommer Nine Ball qui est la cybercriminelle du groupe de braqueuses dans le film *Ocean's 8* (2018) qui est l'unique fille du groupe à s'habiller de façon réellement différenciée (bonnet de rastafari, …). Au sujet de la donnée « Correct », elle figure lorsque le cybercriminel a un style vestimentaire, une apparence physique qui ne se démarque pas des autres protagonistes. Le cybercriminel se fond en quelque sorte dans la masse. C'est le cas avec Karl Koch dans *23* (1998), Ed Porter dans *I.T* (2016), … Quant au critère « Soigné », il correspond au cybercriminel en « col blanc » qui s'habille en costume dans le cadre des œuvres collectées que nous avons analysées. Nous pouvons citer l'antagoniste Raoul Silva dans le film *Skyfall* (2012), Cipher dans *Fast & Furious 8* (2017), …

Une case supplémentaire intitulée « Notes » vient compléter l'ensemble des critères de la grille d'analyse et récapitule l'intégralité des informations collectées lors du visionnage de l'œuvre. Dans la grille d'analyse, les données disposées sur fond vert mentionnent que l'œuvre fait partie d'une série, de légers changements de données s'opèrent donc entre les œuvres concernées car le cybercriminel étudié est le même. Les données marquées d'un fond jaune (ND pour Non Disponible) dans la grille d'analyse indiquent une absence : ses données ne sont pas disponibles dans l'œuvre. Il en est question pour deux œuvres (*Black Mirror / épisode 3 saison 3 : Tais-toi et danse* de 2016, *Ratter* de 2017) notamment dans un cas précis : le(s) cybercriminel(s) ne sont pas directement présenté(s) dans l'œuvre, on ne les voit pas directement à l'écran mais ils agissent par leur(s) acte(s) sur leur(s) victime(s). Nous faisons le choix de conserver ses œuvres dans la grille car elles permettent malgré tout d'obtenir des données importantes comme les actes cybercriminels effectués ce qui est positif pour nos recherches.

2.1.3. Limites du protocole de recherche

Si nous avons construit la grille d'analyse et le corpus avec autant d'objectivité et de rigueur possible, le protocole de recherche possède malgré tous ses limites. A posteriori, nous pouvons les lister successivement.

Nous commençons par celui qui a déjà été explicité, à savoir le fait que toutes les œuvres du corpus ne peuvent-être consultées en intégralité. Certaines données sont alors issues de recherches parallèles et non des œuvres en elles-mêmes suite à une prise de notes pour les

quelques cas concernés. Il est aussi complexe de maintenir constamment une objectivité accrue lorsque nous nous immergeons dans une œuvre cinématographique ou vidéoludique durant l'analyse. Un rappel de l'impartialité et une posture scientifique de tous les instants sont requis, l'évidence est bannie. Le corpus de ce travail se compose d'œuvres qui ont été rassemblées lors des recherches préalables par les méthodes expliquées plus haut ; il est loin d'être exempt que des œuvres peu connues et disposant d'un budget moins conséquent aient été négligé dû à une accessibilité plus restreinte. Enfin, des informations de la grille d'analyse du corpus sont absentes pour quelques films ce qui s'explique par des données non présentes dans les œuvres en question pour diverses raisons déjà évoquées (choix scénaristiques, …).

De même, les limites de la grille d'analyse peuvent-être notifiées. En effet, la grille peut toujours être améliorée pour recueillir davantage de données. Plus de données sont récoltées et plus il y a matière à comprendre et à cerner le(s) représentation(s) du cybercriminel. Des critères supplémentaires peuvent être ajoutés comme la présence du sweat à capuche, l'espace de vie et de travail du cybercriminel dépeint, la finalité de l'acte cybercriminel, la présence ou non de problèmes familiaux antérieurs, ...

2.2. Analyse d'un corpus d'œuvres culturelles

Conformément à l'approche globale, l'analyse du corpus d'œuvres culturelles permet de dresser plusieurs tableaux de données issus de la grille principale regroupant l'ensemble des critères d'évaluation pour les 70 œuvres. Ces différents tableaux permettent de représenter graphiquement les informations obtenues et d'accéder aux données par critère précis. Nous avons fait le choix de retranscrire les données collectées en pourcentages car ceux-ci sont plus évocateurs. De même, les données Non Disponibles (critère ND dans les tableaux et la grille d'analyse principale) ne sont pas affichées sur les différentes représentations graphiques pour des questions de lisibilité.

Nous sommes partis sur 3 représentations graphiques différentes (diagramme vertical à barres, diagramme horizontal à barres, diagramme circulaire, graphique en courbes) pour afficher visuellement les résultats obtenus de la manière la plus évocatrice possible ; ainsi les tableaux correspondants aux graphiques présentés sont à retrouver en Annexes.

Premièrement, nous pouvons présenter les deux graphiques suivants qui contiennent les données relatives au sexe du cybercriminel représenté dans l'œuvre ainsi que le réalisateur(rice) de l'œuvre.

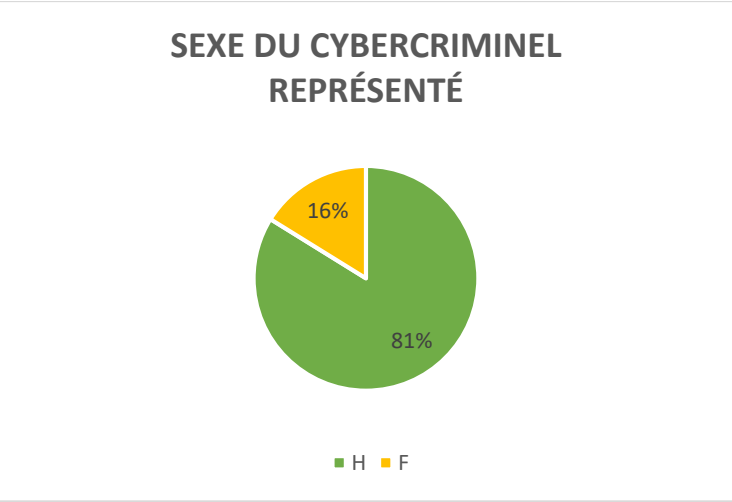


Figure 6 : sexe du cybercriminel représenté dans les œuvres culturelles analysées (H/F)

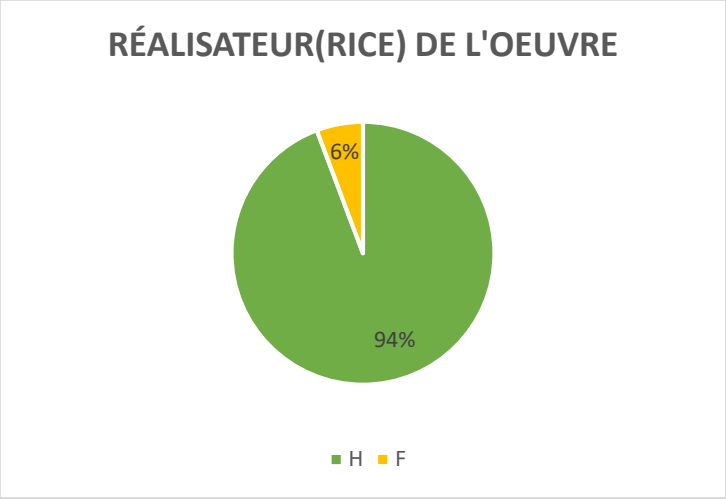


Figure 7 : sexe du réalisateur(rice) des œuvres culturelles analysées (H/F)

Si l'on regarde les résultats, on aperçoit que le cybercriminel représenté au sein des œuvres culturelles collectées est majoritairement un homme (81%). De plus, on constate un comportement similaire quant aux réaliteurs(rices) des œuvres culturelles (94% des œuvres culturelles collectées qui mettent en scène un cybercriminel sont réalisées par des hommes). Il y a une corrélation entre ses deux variables. Nous pouvons dire que le cybercriminel représenté au sein des œuvres culturelles est majoritairement un homme dans des œuvres qui sont pour la plupart réalisées par des hommes. La représentation du cybercriminel est construite essentiellement par des hommes. Les tableaux des données exposées sont disponibles en Annexes (Annexes 1 et 2).

Ces résultats s'expliquent par trois principaux vecteurs :

- les facteurs internes des industries culturelles et notamment du cinéma (la parité hommes/femmes travaillant dans les industries culturelles concernées)

- le stéréotype du geek/informaticien déjà présent depuis de nombreuses années comme le soulève Antonio Casilli (Casilli, 2011) semble perdurer et se lier avec le cybercriminel

- le genre de la profession (la parité d'étudiants hommes/femmes dans les domaines de l'informatique)

Le deuxième graphique que nous dressons ensuite porte sur le nombre de cybercriminels dans les œuvres culturelles étudiées.

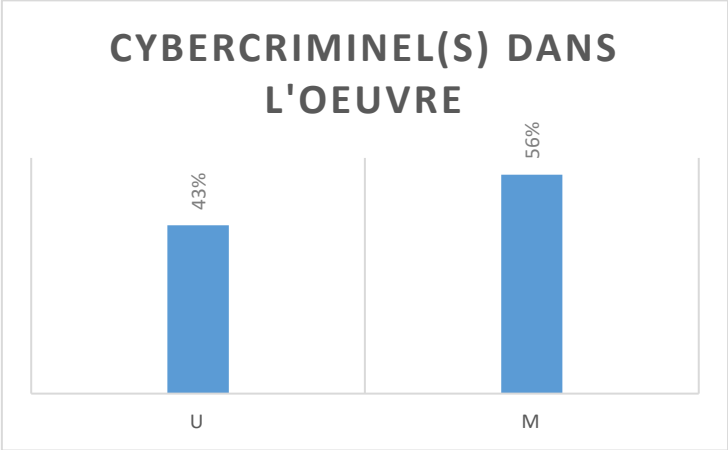


Figure 8 : présence Unique ou Multiple de cybercriminel(s) dans les œuvres culturelles analysées (U/M)

Nous remarquons que dans les œuvres culturelles collectées, il y a majoritairement la présence de plusieurs cybercriminels et non d'un unique. 56% des œuvres font état de cybercriminels. Cette constatation n'est que légère puisque l'on observe un écart de 13% mais elle est toutefois à noter. Ce constat trouve ses sources dans la logique des cybercriminels à s'organiser en groupe comme l'évoque David S. Wall (Wall, 2015). Il y a aussi l'origine propre à « l'ancienne éthique *hacker* » (clubs d'informatique, …) mais également l'actualité médiatique avec l'apparition de groupes comme Anonymous, Lulzsec, … qui constituent une réalité historique factuelle inévitable.

En troisième partie des critères relatifs au cybercriminel représenté, nous nous centrons sur la tranche d'âge du cybercriminel représenté tel que nous l'avons évoqué plus haut. Au vu des résultats, on s'aperçoit que le cybercriminel figure dans deux tranches d'âge : les 15-25 ans

avec 36% de cybercriminels et les 25-50 ans avec 57% de cybercriminels ce qui fait de cette seconde tranche la plus représentative.

La représentation du cybercriminel dans les œuvres culturelles tend à représenter un homme, d'un âge compris entre 25 et 50 ans. Cette représentation se détache de l'idée perçue d'Internet comme le « territoire de la jeunesse » (Casilli, 2011).

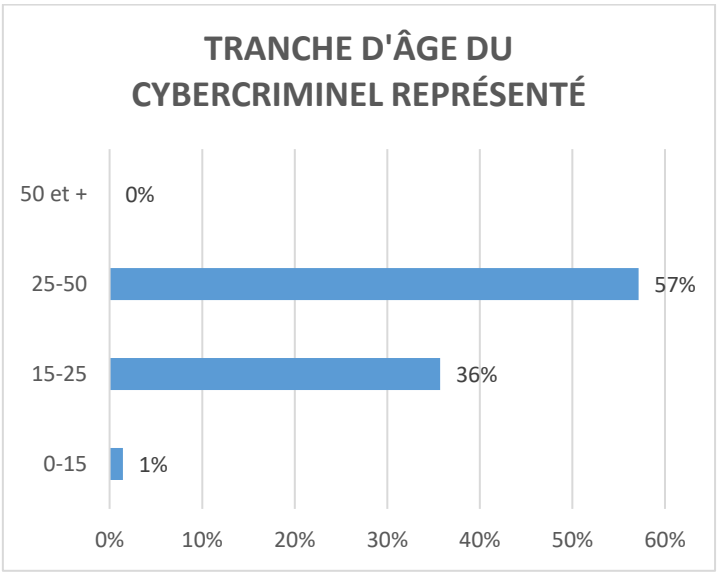


Figure 9 : tranche d'âge du cybercriminel représenté dans les œuvres culturelles analysées

En troisième partie, nous nous sommes penchés sur les résultats obtenus partant du lien ou non entre la profession du cybercriminel représenté et le monde du numérique. En effet, il apparaît nettement que le cybercriminel représenté met à profit ses compétences informatiques au service de sa profession et/ou réciproquement (37% des professions sont liées au numérique). Le cybercriminel représenté dispose d'un ancrage professionnel. Il a été régulier tout au long de la collecte et de l'accès aux œuvres culturelles durant ces recherches de se confronter à l'individu qui mène une double vie entre cybercriminel accompli et technicien informatique « sans histoires ».

La catégorie « Non concernée » dans le tableau correspondant (*cf.* Annexe 5) regroupe les œuvres dont le cybercriminel représenté ne dispose pas d'un emploi officiel et ne peut donc par conséquent pas appartenir à cette seconde analyse du lien entre la profession exercée et le numérique. Il est pertinent d'en tenir compte.

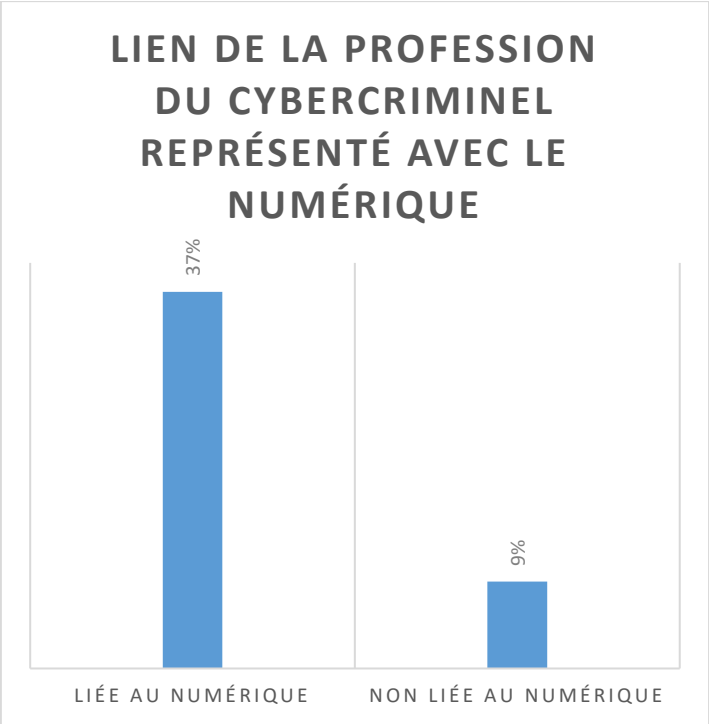


Figure 10 : lien de la profession du cybercriminel représenté avec le numérique dans les œuvres culturelles analysées

Le graphique ci-dessous référence quant à lui la catégorie socioprofessionnelle du cybercriminel. Nous pouvons voir que 50% des cybercriminels représentés sont issus du Niveau agrégé « Autres personnes sans activité professionnelle ». Il est à préciser que conformément aux Niveaux agrégés définis par l'Insee, les « Autres personnes sans activité professionnelle » regroupe de surcroît les étudiants. Le fait est qu'un certain nombre des cybercriminels représentés sont des étudiants (9 pour être exact).

Le cybercriminel tel qu'il est dépeint par l'industrie culturelle est un individu qui vit à part de la société ou un individu qui ne l'a pas encore totalement intégrée pour le cas précis de l'étudiant. Des œuvres culturelles collectées présentent un individu sans emploi « officiel » qui vit grâce à l'économie parallèle et les bénéfices engrangés par ses activités cybercriminelles. Il y a ici une dimension qui fait appel à « l'économie du cybercrime » telle que développée par Solange Ghernaouti et Arnaud Dufour ; dimension qui a pleinement été intégrée à la représentation du cybercriminel dans les œuvres culturelles (Ghernaouti et Dufour, 2017).

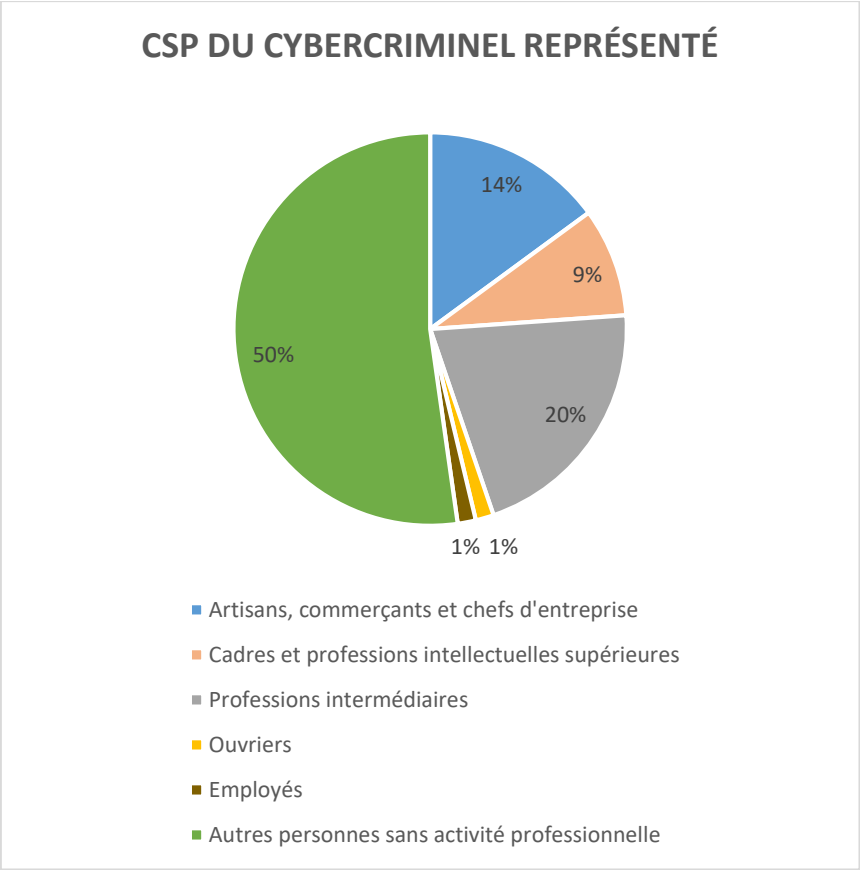


Figure 11 : catégorie socioprofessionnelle du cybercriminel représenté dans les œuvres culturelles analysées

Dans les œuvres culturelles collectées pour notre étude, nous avons inscrit tous les actes cybercriminels effectués par l'individu observé dans chaque œuvre. Conformément aux données du graphique à courbes (*cf.* Figure 12), nous pouvons remarquer des actes cybercriminels récurrents dans toutes les œuvres analysées. Des cybercrimes ont tendance à être représenté souvent de manière formelle à l'écran. En premier lieu, on retrouve le vol de données dans presque 25% des cas. En d'autres termes, en tant que spectateur, nous ne savons pas exactement (avec quelles techniques, ni par quelles attaques informatiques) comment le cybercriminel s'est fourni les données qu'il a en sa possession. Nous avons uniquement connaissance que ces données digitales (de tout type : documents audiovisuels, documents textuels, …) n'ont pas à être en sa possession et que celui-ci les a obtenu illégalement par l'intermédiaire du numérique. En second lieu, la prise de contrôle en temps réel d'un système informatique à distance (9%). Par système informatique, nous entendons tous les supports numériques existants à ce jour : smartphone, tablette, ordinateur, serveur, … Cette donnée est établie dès lors que le cybercriminel représenté dans l'œuvre prend le contrôle en temps réel de la machine de sa victime à distance : cela se traduit notamment par le pointeur de la souris qui se déplace automatiquement sans action de l'utilisateur légitime, de commandes entrées

automatiquement dans la console du système d'exploitation, ... En un troisième lieu, on retrouve le détournement de caméras de vidéosurveillance (8%), nous observons sur l'écran du cybercriminel une prise de contrôle des caméras de surveillance d'un ou plusieurs lieux en temps réel. Il est intéressant de voir que des attaques cybercriminelles précises telle que le *phishing* ou bien le *phreaking* ne sont que très peu représentées formellement dans les œuvres culturelles qui mettent en scène un cybercriminel. La représentation du cybercriminel s'axe donc sur un individu qui dérobe illégalement des données, qui prend le contrôle à distance d'un système informatique et qui sait avoir accès aux caméras de surveillance.

D'autres cybercrimes ressortent également de cette étude mais de façons moins fréquentes que les attaques précédemment citées. Parmi celles-ci, nous trouvons : la création de logiciels malveillants (7%), le détournement de fonds (sans pratique du *carding*) également à 7%, la géolocalisation de systèmes informatiques (4%), ...

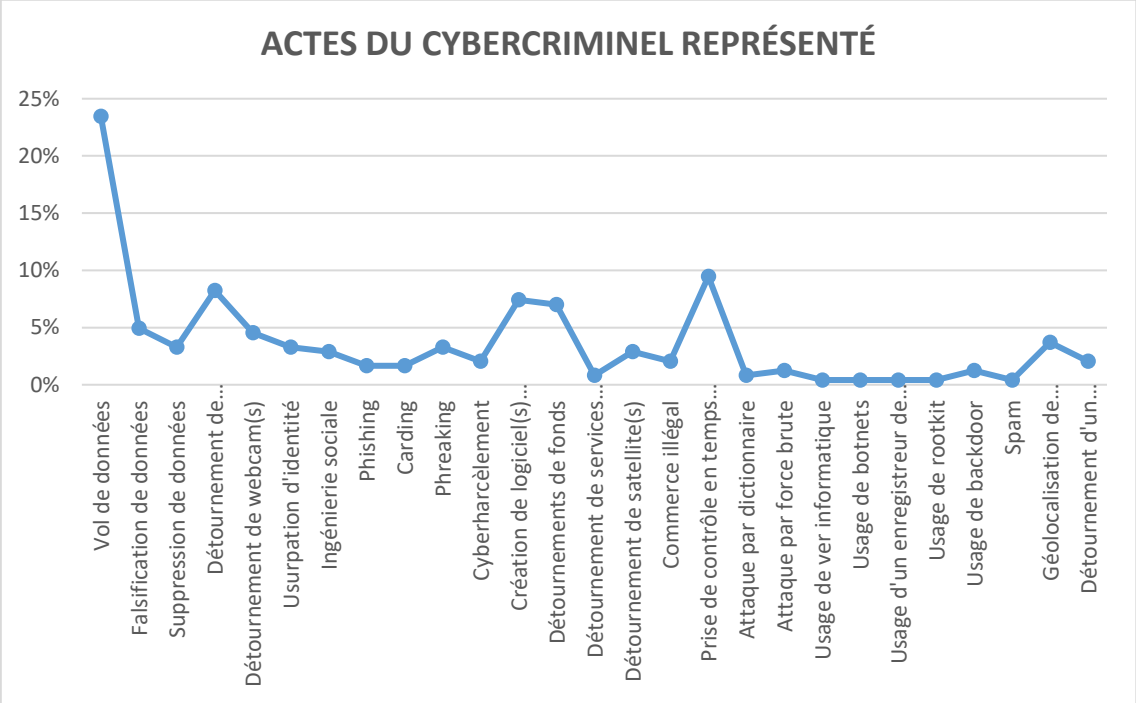


Figure 12 : actes du cybercriminel représenté dans les œuvres culturelles analysées

Par la suite, nous avons classé le lien social du cybercriminel représenté. Nous obtenons des résultats partagées en trois types relations sociales (*cf.* Figure 13 et Annexe 8) : 40% des cybercriminels représentés ont un lien social réel, 27% des cybercriminels représentés ont un lien social réel et virtuel, 13% des cybercriminels représentés ont un lien social composé de leur famille et de relations réelles. Le cybercriminel représenté au sein des œuvres culturelles collectées n'est finalement pas individu si solitaire comme nous pouvons parfois l'entendre.

Ceux-ci ont au moins un contact réel, physique et régulier avec des individus. Ce contact passe par des discussions, une communication quotidienne avec leurs collègues de travail, ... Bien que ces échanges sociaux ne soient pas nécessairement longs sur la durée temporelle ou que l'importance accordée aux individus soit moindre, il n'empêche que ces contacts ont lieu et participent à l'instauration d'un lien social même minime par de la communication. Lorsque le lien social est virtuel, il est complété avec du lien social réel. Cette configuration du lien social existante pour le cybercriminel représenté dans les œuvres culturelles se justifie partiellement pour une raison scénaristique : il est particulièrement complexe de dépeindre un cybercriminel sans aucune relation sociale à l'écran, aussi bien pour des œuvres cinématographiques que télévisuelles ou encore vidéoludiques. Une œuvre doit pouvoir susciter l'attention de son public et il est difficile d'y parvenir avec si peu d'informations visuelles dévoilées.

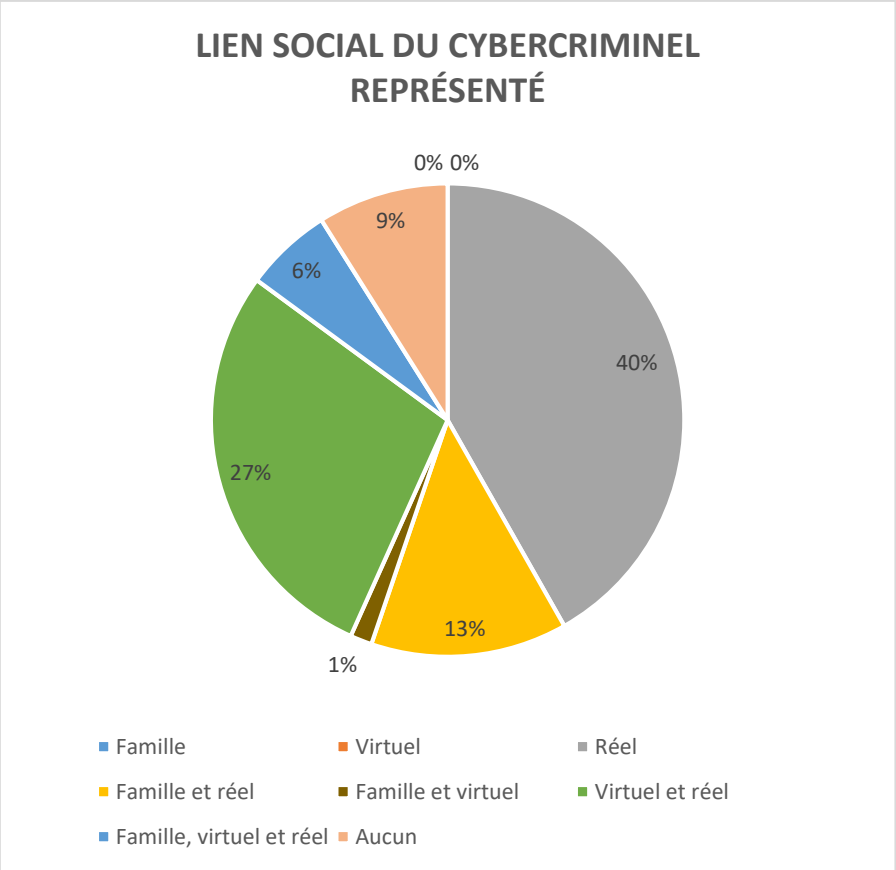


Figure 13 : lien social du cybercriminel représenté dans les œuvres culturelles analysées

Pour terminer sur cette phase d'analyse, le style vestimentaire, l'apparence physique du cybercriminel représenté est classée. Nous dénombrons 66% d'individus au style vestimentaire et à l'apparence physique correcte, 19% d'individus au style vestimentaire et à l'apparence physique soignée et 10% d'individus au style vestimentaire et à l'apparence physique atypique. Nous le rappelons mais il n'est pas question d'un jugement ou d'une discrimination mais

uniquement l'observation des différences qui peuvent s'opérer dans les représentations physiques, esthétiques du cybercriminel. Ces résultats dévoilent trois caractéristiques sur la représentation du cybercriminel au sein des œuvres culturelles : c'est le plus souvent un individu qui se fond dans la masse et qui peut correspondre à n'importe quel concitoyen ; dans d'autres œuvres moins nombreuses, c'est un cybercriminel « en col blanc » conformément aux « criminels en cols blancs » que rapporte Franck Guarnieri et Éric Przyswa avec leurs recherches sur la cybercriminalité et la contrefaçon (Guarnieri et Przyswa, 2012) ; enfin dans une minorité de cas, il s'agit d'un individu qui se différencie visuellement et laisse transparaître l'appartenance à genre, à un mouvement, à un style.

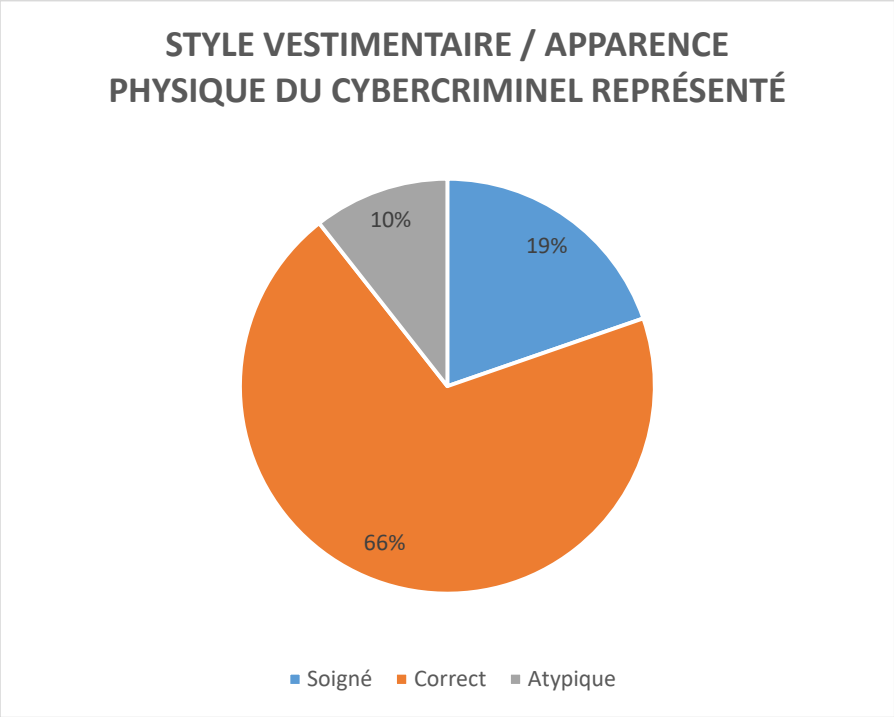


Figure 14 : style vestimentaire / apparence physique du cybercriminel représenté dans les œuvres culturelles analysées

2.3. Entretiens avec des professionnels du numérique

Les productions issues des milieux culturelles donnent des approches quant au sujet de la représentation du cybercriminel pour le grand public. En complément de ces données et à juste titre de comparaison, le secteur des professionnels du numérique et des professionnels de la cybercriminalité ouvre la voie à d'autres perspectives qu'il nous faut sonder et qui complètent les représentations et stéréotypes concernant notre objet d'étude. Les professionnels, de par leur travail de terrain, s'affranchissent-ils de ses représentations ? Ont-ils de tous autres schémas de pensées ?

En termes méthodologiques, nous nous tournons vers une première prise de contact par messagerie électronique. Une fois cette prise de contact établie, compte-tenu de la situation et du contexte de chacun pendant la période de confinement liée à la crise du COVID 19, nous partons sur un formulaire à compléter en ligne ou directement sur un entretien en visioconférence ; l'entretien en visioconférence est cependant privilégié systématiquement car l'échange communicationnel et son instantanéité sont plus propices pour faire ressortir des informations. Toutefois, le questionnaire propose également l'éventuelle opportunité de réaliser un entretien dans les dernières questions afin de maximiser le taux de retours. Pour mettre en œuvre ce travail, nous dressons plusieurs questions choisies murement afin de nous apporter des éléments de réponse tout en veillant à laisser une place prépondérante à la spontanéité au sujet des entretiens en visioconférence spécifiquement. Les questions du formulaire sont similaires à celles des entretiens dans l'optique de conserver une cohérence et une équité durant l'ensemble du protocole de recherche. Sous un angle technique, les entretiens en visioconférence ont été enregistrés sous format vidéo et sont disponibles depuis un lien en Annexes (*cf.* Annexes 15 et 16 pour le format vidéo, Annexes 18 et 19 pour la retranscription). Ceux-ci ont été réalisés avec le logiciel dédié Skype. Les questions sont quant à elles directement disponibles via le formulaire Google Forms depuis un lien d'accès en Annexes (*cf.* Annexe 14) mais également au travers de captures d'écrans (*cf.* Annexe 10, 11 et 12).

Les professionnels qui ont accepté de participer à ce travail de recherche ont été contactés par différents moyens. Premièrement, nous avons pris contact avec les intervenants professionnels du Master AMINJ Création de Projets Numériques (CPN) à l'UFR SHS de Metz, intervenants qui ont gracieusement accepté de participer à l'enquête. Dans un second temps, nous avons recherché des intervenants en cybercriminalité du côté du salon Grand Est Numérique (GEN) qui a lieu chaque année au sein de la ville de Metz et qui propose à tous les acteurs du numérique des temps d'échange. Des publications sur les réseaux sociaux invitant les professionnels du numérique à compléter le formulaire (particulièrement sur le réseau social LinkedIn pour son aspect professionnel) ont été mené. Enfin, plusieurs messages électroniques ont été envoyés à des responsables de formation dans le domaine de l'informatique et de la cybersécurité. Nous avons aussi sollicité chaque professionnel intéressé par notre enquête à partager le lien du formulaire à son propre réseau.

Passons au début du formulaire où l'on retrouve deux premières questions génériques précisant la profession occupée par la personne interrogée. Ces deux questions visent également à

introduire une communication stable avec l'interlocuteur en début d'échange avant d'aborder des questions plus précises. Par la suite, nous tentons d'en savoir davantage sur les perceptions des individus sondés en les invitant à donner :

- Leur propre définition de ce qu'est pour eux la cybercriminalité ;
- S'ils établissent une distinction entre les termes « *hacker* », « cybercriminel » et « pirate » ou d'autres dénominations qui leur viendraient à l'esprit (importance du caractère spontané des entretiens en visioconférence) ;
- Des informations relatives à leur(s) perception(s) du/des cybercriminel(s) en lien avec les données de la grille d'analyse des œuvres culturelles (milieu social, âge, actes malveillants, …) ;
- Les influences qui pourraient impacter sur leur(s) représentation(s) : terrain, œuvres culturelles, …
- Leur avis sur la réflexion autour d'un profil type au travers de quatre affirmations (*cf.* Annexe 11)/

Notre formulaire se finalise alors sur la demande d'entretien en visioconférence accompagné de quelques informations supplémentaires de contact.

Parmi l'ensemble des retours, il convient de s'arrêter sur certaines réponses particulièrement enrichissantes pour notre travail de recherche.

Quatre professionnels ont répondu à notre questionnaire :

- un juriste spécialisé en Droit pénal chargé de la conception de la doctrine de la Police Judiciaire en matière de cybercriminalité ;
- un policier investigateur en cybercriminalité ;
- un ingénieur en cybersécurité pratiquant en indépendant ;
- un directeur technique au sein d'une SSII[36].

[36] Entreprise de Services du Numérique (ESN, anciennement SSII).

Les deux premières personnes sondées fondent leur définition de la cybercriminalité sur les « systèmes de l'information et de communication », « les techniques de l'information ». À partir de cet élément, la cybercriminalité est définie comme un ensemble de pratiques hormis pour la personne juriste qui caractérise spécifiquement la cybercriminalité par ce qui est entendu au nom de la loi par le terme d'« infractions pénales ». Dans le cadre du droit, la cybercriminalité recouvre toutes les attaques produites « au moyen ou à l'encontre d'un système […] ». L'individu ingénieur en cybersécurité parle « d'utiliser les outils cyber » pour nous expliquer la définition de la cybercriminalité. Cela nous renvoie directement à l'usage des « cybermots » du côté de Stéphane Leman-Langlois ainsi que de l'usage du préfixe « cyber » chez Nicolas Arpagian, des recherches vues plus tôt dans ce travail. Le directeur technique introduit et encadre sa définition autour de la notion de « réseau » spécifiquement. L'individu juriste marque une distinction entre les termes « *hacker* », « cybercriminel » et « pirate » car pour lui, un *hacker* peut être associé ou non à chercheur en sécurité informatique. L'enquêteur en cybercriminalité, l'ingénieur en cybersécurité et le directeur technique n'opèrent pas de fragmentation au quotidien en ce qui les concerne. Sur les actes malveillants perpétrés selon notre typologie des actes cybercriminels définie pour la grille d'analyse des œuvres culturelles, il est intéressant de noter qu'aucune des personnes sondées ne reconnaît le détournement de satellite(s) : cette activité est le pur produit de l'imagination des œuvres culturelles car on retrouve cette action dans plusieurs œuvres (*cf.* Figure 12 et Annexe 7). À l'inverse, tous les professionnels sondés font état du *phishing* (hameçonnage) suivi du vol de données, de l'attaque par force brute, de l'usage de botnet et du spam à parts égales (80%). L'ingénieur en cybersécurité et le directeur technique décrivent leur stéréotype du cybercriminel respectif comme étant un homme jeune avec pour le premier une caractéristique propre de localisation géographique se tournant vers les pays en voie de développement ; et pour le second, un autodidacte solitaire et talentueux. Les deux premières personnes interrogées avec le formulaire s'accordent sur deux points essentiels : leur représentation du cybercriminel est influencée par les œuvres culturelles (on nous cite notamment l'œuvre cinématographique *Cybertraque* sortie en 2000 et présente dans notre grille d'analyse), ce qui confirme le postulat défendu dans notre travail, mais également par leur travail de terrain en tant que professionnels. Une affirmation parmi les 5 proposées ressort en une approbation commune (*cf.* Annexe 11) : « il y a souvent des traits communs chez les cybercriminels ». À l'inverse, une autre affirmation se détache en une désapprobation commune : « il y a des traits communs dans les parcours de vie ».

Nous tenons à porter une attention particulière à la contribution de Mme Anne Souvira, commissaire divisionnaire et chargée de mission aux questions relatives à la cybercriminalité au sein du cabinet du Préfet de Police de Paris qui participe au Groupe de Travail Interministériel de lutte contre la cybercriminalité mis en place depuis 2013. Mme Anne Souvira est en effet une experte de par une carrière importante et une large expérience sur la cybercriminalité puisqu'elle a notamment dirigé la Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information (BEFTI). Mme Anne Souvira a accepté de répondre à notre formulaire et nous en avons retiré des informations précieuses. Elle définit la cybercriminalité comme suit: « les infractions commises contre les réseaux et systèmes d'informations ou commises en utilisant ces réseaux et infrastructures (*cf.* Rapport de Marc Robert intitulé 'Protéger l'Internaute'[37]) ». En outre, Mme Anne Souvira reconnait l'aspect sémantique particulier des termes « hacker », « cybercriminel » et « pirate » mais s'en tient aux faits juridiques en mentionnant la Loi Godfrain du 5 janvier 1988 qui est la première loi française portant sur la fraude informatique. Sur la question du stéréotype du cybercriminel, Mme Anne Souvira note « les difficultés d'accès à la preuve numérique » qui rendent les arrestations de cybercriminels que peu fréquentes ainsi que l'absence d'études à ce sujet du côté de la Police. Elle décrit le stéréotype du cybercriminel comme un homme jeune bien que les plus redoutables soient plus âgés. Enfin, Mme Anne Souvira est en désaccord avec l'affirmation suivante : « il y a des traits communs dans la psychologie » et approuve l'affirmation : « je pense qu'il y a une grande hétérogénéité de profils chez les cybercriminels ». Son apport à notre enquête a été précieux et nous la remercions encore pour le temps accordé.

Lors des entretiens en visioconférence (*cf.* Annexes 15, 16, 18 et 19), M. Franck Bettanier, chargé de communication au sein du Ministère des Armées évoque une distinction entre le terme « *hacker* » et le terme « cybercriminel » car dans le cadre de sa profession les *hackers* ne sont pas nécessairement des cybercriminels car ils travaillent à « dérober des informations » sur de potentielles menaces terroristes. Sans entrer dans des questionnements politiques, nous remarquons qu'il existe des ambivalences du terme « cybercriminel » en fonction de qui bénéficie des actions menées. Par ailleurs, M. Franck Bettanier évoque sa représentation du cybercriminel comme un homme jeune (« entre 20 et 35 ans »), stéréotype qu'il lie aux informaticiens qu'il rencontre dans le cadre de sa profession et qui sont des hommes pour une grande majorité.

[37] http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf

Dans le second entretien, M. Nicolas Chevrier, gérant de l'agence de communication Noutan, divise la cybercriminalité entre deux aspects : d'une part le côté malveillant avec les attaques informatiques et de l'autre une vision particulièrement positive qui se traduit par les œuvres culturelles de science-fiction. En outre, il ne souligne aucune différence pour sa part lorsqu'il utilise les termes « cybercriminel », « *hacker* » et « pirate » : conformément à ce qui a pu être observé dans notre état de l'art avec les travaux des chercheurs, il y a eu des évolutions étymologiques qui se sont développées sur l'usage des termes. M. Nicolas Chevrier énonce le *phishing* (hameçonnage) en principale attaque cybercriminelle ainsi que les attaques de serveurs Web, menaces qu'il a pu fréquemment rencontrer dans sa profession. Ces actes cybercriminels ne sont pourtant que très peu dépeints dans les œuvres culturelles (*cf.* Figure 12 et Annexe 7). Tel que vu plus tôt avec les réponses du formulaire en plus des éléments ci-présents traduits par M. Nicolas Chevrier, le *phishing* est une attaque bien identifiée et fréquente chez les professionnels du numérique et de la cybersécurité, pourtant elle n'est que peu présente dans le contexte de la représentation du cybercriminel dans les œuvres culturelles. M. Nicolas Chevrier explicite ensuite ses représentations du cybercriminel, dont un homme jeune « geek » ainsi qu'un second profil plus âgé « en costume cravate », qui s'éloignent de sa réalité professionnelle mais qui se conforment aux œuvres culturelles qu'il a pu visionner, lire, …

Pendant les deux entretiens en visioconférence, les deux personnes sondées ont également approuvé les affirmations : « il y a souvent des traits communs chez les cybercriminels » ; « je pense qu'il y a une grande hétérogénéité chez les cybercriminels ». Ils ont tous deux désapprouvé l'affirmation : « il y a des traits communs dans les parcours de vie ». Nous constatons sur ses trois affirmations des résultats similaires aux réponses du formulaire.

Nous ne pouvons donc pas déclarer avec certitude qu'il existe à ce jour un profil type du cybercriminel nettement identifiable du côté des professionnels en cybercriminalité et des professionnels du numérique si nous nous en tenons à ces éléments de réponse. Les professionnels de la cybercriminalité se rattachent davantage aux définitions juridiques. Nous pouvons néanmoins affirmer que l'ensemble des acteurs du monde professionnel ont conscience de l'hétérogénéité de cette figure numérique tout en soulignant des points de convergences. Les données collectées sont particulièrement hétérogènes et éparses. L'impact des œuvres culturelles et du milieu professionnel sur les représentations est toutefois bien présent.

3. Frontières mouvantes, vers de nouvelles figures

Après une mise en perspective des données collectées depuis la grille d'analyse, nous pouvons dresser les constats et les remarques suivantes.

3.1. Trois époques d'imaginaires

Nous distinguons trois périodes du cybercriminel représenté qui se dessinent après l'ensemble des œuvres visionnées et étudiées.

3.1.1. La cybercriminalité en trois dimensions (1980-1995)

Dans les premiers films sur Internet, à partir du début des années 1980, le cybercriminel est mis en scène dans un environnement en trois dimensions représentant Internet. Nous notons dans la grille d'analyse : Kevin Flynn avec CLU dans *Tron* de 1982, Neo dans la trilogie *Matrix* qui paraît en 1995, … Non présent dans la grille d'analyse pour l'absence d'un cybercriminel dans l'œuvre mais tout aussi évocateur, *Johnny Mnemonic* de 1995 également. L'aspect science-fiction prédomine nettement. Les œuvres cinématographiques pionnières sur le sujet se diversifient également par la mise en scène des actes cybercriminels qui varient grandement en fonction de l'esthétique choisie par les réalisateurs : de grandes libertés sur l'imaginaire sont prises (choix de formes aux couleurs prononcées, lumières, scintillements, formes en trois dimensions, hologrammes, …). Cette première période à laquelle s'associe cette première représentation du cybercriminel s'explique avec ce que nous avons pu développer précédemment dans l'état de l'art : le mouvement cyberpunk et l'émergence ainsi que la démocratisation progressive d'Internet durant ces mêmes années. Cette première représentation du cybercriminel s'inscrit pleinement dans la représentation d'Internet en elle-même. Il fallait trouver les moyens de représenter de façon attrayante cette nouvelle catégorie d'individus liés à une technologie encore bien méconnue. Les œuvres citées dépeignent un futur dystopique, elles sont issues pour certaines directement d'œuvres littéraires cyberpunk et utilisent les codes de ce mouvement en plus de faire apparaitre le type « cyberfilm ». Bien évidemment certains films échappent mieux aux standards cinématographiques de leur période contrairement à d'autres. Ces films concernés s'affranchissent déjà de la représentation du cybercriminel qui semble se mettre en place dans le cadre de la représentation d'Internet de façon plus globale en un environnement tridimensionnel. Dans *WarGames* (1983), la représentation des actes cybercriminels reste correcte et relativement réaliste (le jeune David Lightman entre des instructions dans son programme sur l'ordinateur qui lui répond, il utilise également un modem acoustique qui est un des outils d'origine du *phreaking*). Nous ajoutons aussi John Connor dans

Terminator 2 : Le Jugement dernier sorti en 1991 qui détourne un Distributeur Automatique de Billets (DAB, *ATM*) sur une attaque par force brute depuis une carte bancaire dérobée à l'aide de son ordinateur portable Atari Portfolio.

3.1.2. Le cybercriminel à son bureau (1995-2000)

Survient ensuite une période (milieu/fin des années 1990) où l'on va retrouver les techniques cybercriminelles plus réelles, mieux représentées, avec encore des défauts mais moins exagérées qu'auparavant : les cybercriminels ont quitté leur espace imaginaire et se retrouvent désormais à leur bureau ; la représentation de la technique reste encore faussée avec des « *Access Denied* », « *Access Granted* » affichés fréquemment sur les écrans cependant la représentation de la technique tend à s'améliorer (*Traque sur Internet* de 1995 en est un bon exemple). L'apparition des lignes de codes se démocratisent, elles défilent toutefois à des vitesses fulgurantes et s'en suivent de cybercriminels qui martèlent leur clavier bien trop rapidement (Kevin Mitnick dans *Cybertraque* en 2000). Le cybercriminel est dépeint comme un être à part, vivant séparé de la société ou tout du moins en conflit avec celle-ci : dans *23* sorti en 1998, Karl Koch est obnubilé par la théorie complotiste des Illuminatis au point d'en perdre la raison, il vit dans son microcosme.

3.1.3. La représentation contemporaine du cybercriminel (2000 – …)

À partir des années 2000 et jusqu'à aujourd'hui, les traces de cette seconde période sont encore présentes dans certaines œuvres cinématographiques (*Opération Espadon* sorti en 2001 avec le personnage de Stanley Jobson, *Firewall* daté de 2006, ...) mais la représentation fidèle du cybercriminel s'affine puisque les méthodes passées ne fonctionnent plus aussi bien. L'accès à l'information sur les cybercriminels s'est démocratisée, de même que l'accès aux technologies du numérique. Le grand public ne dispose plus des mêmes attentes et sait se défaire des représentations antérieures qui deviennent alors non crédibles. La représentation de l'acte cybercriminel atteint notamment un niveau jamais égalé en matière de réalisme au sein de la série télévisuelle *Mr. Robot* diffusée pour la première fois en 2015 sur la chaîne *USA Network*. Dans cette œuvre télévisuelle, le sens du détail et l'aspect technique de l'acte cybercriminel sont traduits d'une grande justesse : le code n'est plus simplement présent pour imager la narration mais ajoute de l'information, les outils utilisés ainsi que les lignes de commandes entrées dans les scènes sont fidèles à la réalité (terminal GNU/Linux, …). Personnage central de l'œuvre, nous voyons sans artifices Elliot Alderson passer du temps sur son ordinateur comme le ferait n'importe quel internaute. Les œuvres cinématographiques actuelles n'hésitent

pas à directement montrer des interfaces logicielles sur les écrans avec plus ou moins de justesse : soit en plan rapproché (*The Social Network* paru en 2010, *Who Am I: Kein System ist sicher* de 2014) ou bien entièrement incorporées à l'écran (*Open Windows* sorti en 2014). Dans *The Social Network* (2010), Mark Zuckerberg détourne une quantité importante de photographies en passant par les dossiers situés dans les serveurs Apache de sites Web. Il utilise également un script pour automatiser ses actions dans le but de gagner du temps. Nous observons la pratique simultanément et comprenons comment cela se traduit sur l'ordinateur. La représentation du cybercriminel est profondément divergente avec ce qui se faisait plus communément une dizaine d'années auparavant. Dans *Open Windows* (2014), l'œuvre cinématographique se compose de ce que voit le personnage principal sur son écran d'ordinateur. Nous avons un retour vidéo de sa webcam et assistons au piratage de son ordinateur en ne voyant que l'écran. L'œuvre cinématographique prend intégralement place au travers des supports numériques (caméras de smartphone, webcam, …).

Parallèlement d'autres œuvres cinématographiques conservant les représentations des années 1995-2000 (*James Bond : Skyfall* de 2012, *Fast & Furious 8* de 2017, …) projettent toujours des interfaces logicielles et des lignes de code fantasmées pour représenter l'acte cybercriminel. Cet aspect continue de jouer considérablement sur la perception du public au sujet du cybercriminel et façonne sa représentation. Q, personnage qui fournit les armes de l'agent britannique James Bond montre à celui-ci le virus de l'antagoniste Raoul Silva sous forme d'une structure polymorphique dans *James Bond : Skyfall (2012)*. En outre, le stéréotype du cybercriminel solitaire est encore bien marqué aujourd'hui (*Aux yeux de tous* paru en 2012, *Mr. Robot* de 2015, *I.T* diffusé en 2016). Dans *I.T* (2016), le cybercriminel Ed Porter vit seul à son domicile sans côtoyer personne en dehors de son travail, il n'a pas de relations amicales ni mêmes familiales. Suite à une enfance difficile et des problèmes psychologiques, il n'est pas en capacité de faire la différence entre une relation professionnelle et amicale avec son directeur ce qui le conduit à des périodes de souffrance, à la rupture de ses liens sociaux accompagnée de moments gênants pour les personnes qui l'entourent.

3.2. Du justicier au soldat

3.2.1. Internet comme lieu de terreur

Plus récemment, Internet est aussi utilisé comme un vecteur de peur dans les œuvres mettant en scène un ou des cybercriminels (*Getaway* sorti en 2013, *Ratter* de 2015, *Black Mirror / épisode 3 saison 3 : Tais-toi et danse* diffusé en 2016, *Assassination Nation* paru en

2018). Le cybercriminel intègre à la perfection l'acteur de cette peur, son incarnation physique. Dans *Black Mirror / épisode 3 saison 3 : Tais-toi et danse* (2016), le(s) cybercriminel(s) n'est pas montré à l'écran pourtant la représentation véhiculée est particulièrement forte et porteuse de sens. La représentation physique du cybercriminel dans les œuvres n'est d'ailleurs pas nécessaire pour construire la représentation, les actes malveillants et l'absence photographique parlent à eux seuls. Le(s) cybercriminel(s) dans *Black Mirror* fait preuve d'une grande perversité. Ces actes visent à faire le mal, à faire souffrir l'autre en nous rappelant l'importance des données numériques : on est dans un cas typique de cyberharcèlement.

Compte tenu de tous ce nous avons pu observer, nous pouvons structurer 4 représentations récurrentes du cybercriminel dans les œuvres culturelles étudiées lors des recherches ; représentations qui se lient aux différents statuts qui ont émergé pour les *hackers* (Dagiral, 2008) :

- Le cybercriminel « braqueur », le cybercriminel « financier » ;

  Présenté en *white hat* bien que son objectif final ne rend pas service au bien commun, il fait cela pour l'argent et se présente comme « le geek » de l'équipe (Livingston Dell dans *Ocean's Eleven* de 2001, Lyle dans *Braquage à l'italienne* sorti en 2003, Rio dans La *Casa de Papel* diffusée en 2017, …).

- Le cyberterroriste ;

  Il recherche soit le chaos (il tend à faire s'effondrer la société) soit l'argent ; il incarne l'antagoniste de l'œuvre et se comporte en ce sens, en *black hat* (Travis Dane dans *Piège à grande vitesse* sorti en 1995, Will Stiles dans *Net Force* dévoilé en 1999, …).

  Tout comme nous avons pu voir l'apparition du type « cyberfilm » pour désigner des œuvres culturelles, le cyberterroriste dans les œuvres observées prend place dans les œuvres du genre techno-thriller où il est question d'une menace terroriste technologique (œuvres littéraires de Tom Clancy adaptées au cinéma, …).

- Le cyberjusticier ;

  Son combat suscite l'empathie, il vise à rétablir la justice, l'égalité. Le cyberjusticier agit pour le bien malgré des moyens illégaux, c'est un *white hat* (Nicholas Hathaway dans *Hacker* paru en 2015, …).

- Le cyberharceleur ;

  Il cherche uniquement à faire souffrir un ou des individus pour son plaisir en se comportant en *black hat* (*Ratter* de 2015, …).

Nous voyons que la représentation du cybercriminel évolue chronologiquement au rythme de la représentation d'Internet, de sa démocratisation et des avancées technologiques mais pas uniquement car des représentations persistent. Le cybercriminel dans les œuvres culturelles est modelé sur plusieurs comportements, sur plusieurs traits de caractère qui dépendent du genre de l'œuvre (thriller, comédie, drame, ...). Ces différentes représentations puisent également leurs sources dans différents mouvements culturels (cyberpunk, …), dans l'actualité (masques du collectif Anonymous issus de Guy Fawkes, …).

3.2.2. Les soldats de l'ombre

Sous le titre de son article « La cyber-guerre : un fantasme qui fait vendre », Daniel Ventre est l'un des premiers chercheurs à s'interroger sur la « figure combattante » du cyber-guerrier et sur les fantasmes qu'elle engendre. Il tente de déconstruire cette image qui se lie avec celle du cybercriminel car l'auteur rend compte de multiples figures à la suite de ses lectures scientifiques. « Le simple citoyen, de chez lui, à partir de son propre ordinateur ou sur son mobile, peut participer aux guerres, y tenir un rôle non négligeable » (Ventre, 2012 : 40). Il part de ce postulat avant de dresser deux principales figures existantes du cyber-guerrier : les cyber-guerriers étatiques et les cyber-guerrier non-étatiques. C'est cette dernière qui va principalement nous intéresser. Les *hackers*, les *hacktivistes* et les cybercriminels sont représentés par cette notion comme l'indique l'auteur, ce qu'il explique par des situations concrètes : « […] depuis le début des années 2000 la mobilisation de compétences civiles non-étatiques chinoises au sein de milices dirigées par l'armée, l'action de groupes de *hackers* (voire de la cybercriminalité), parfois qualifiés de cyber-guerriers, agissant au service des intérêt de l'État » (Ventre, 2012 : 42). L'auteur parle principalement de ce fait avec l'Estonie, la Chine et Israël. Ces exemples se manifestent pour des raisons politiques précises : une volonté de sous-traitance provenant des états concernés, « le besoin de réguler une population de hackers constituant une menace », … Ce sont ces phénomènes qui continuent de faire progresser la figure du « cyber-guerrier » tout en l'inscrivant conjointement à la cybercriminalité. L'actualité récente en est la cause majeure.

La démocratisation des mots « cyberattaque », « cyberarme », « cyberdéfenseur » témoigne de l'arrivée d'une sémantique militaire pour désigner tous les éléments qui recouvrent de près ou de loin la cybercriminalité. D'une manière, nous revenons aux sources d'Internet avec le réseau ARPANET développé militairement. Cependant, on se situe dans une logique d'attaque et plus de défense. En septembre 2019, la franchise mondiale de jeux vidéo *Call of Duty* dévoile le mode de jeu multijoueur « Cyber Attaque » au sein duquel les joueurs s'affrontent pour installer un dispositif IEM dans la base ennemie (dispositif à Impulsions ÉlectroMagnétiques qui détruit les appareils électroniques). *Call of Duty* étant une série de jeux vidéo FPS (*First-person shooter*), les joueurs incarnent des soldats et le dispositif IEM est utilisé en tant qu'arme militaire. À la suite de ce récent exemple culturel, soulignons aussi les « risques cyber » affichés sur le site officiel du gouvernement français[38] (*cf.* Figure 5) qui incluent la cybercriminalité, l'atteinte à l'image, l'espionnage et le sabotage. Des catégories que nous pouvons facilement remettre en question compte tenu des recherches que nous avons explorées dans ce travail.

Figure 15 : les risques majeurs à la nation française (Source : gouvernement.fr)

À cela, les attaques DOS par l'utilisation de *botnets* participent à la reconstruction de la figure du cybercriminel en « cyber-guerrier ». Les *botnets* sont perçus comme des soldats robotisés, la dimension massive de ses attaques se schématise par un cybercriminel contrôlant une « armée de machines » derrière son seul ordinateur qui agit en tour de contrôle. Ces attaques réseautées suscitent le discours de par leur grande portée d'action (échelle mondiale) et la dispersion géographiques des ordinateurs responsables. « Des ordinateurs *zombies* peuvent être activés à distance […]. Ces machines *zombies* forment des réseaux de plusieurs dizaines, voire des centaines de milliers de machines […] » (Ghernaouti et Dufour, 2017 : 103). Ces actes cybercriminels sont le résultat de processus d'une grande rigueur, volontairement coordonnés et préparés en amont.

[38] https://www.gouvernement.fr/risques/risques-cyber

Les cybercriminels s'organisent également davantage en groupe comme nous l'avons étudié. Cette dimension plus structurée entraine cette nouvelle représentation qui est comparable à des milices. Ces individus d'un ordinaire plus isolé dans leurs actions se sont militarisés en mettant en commun leurs compétences et techniques tout en se professionnalisant.

Historiquement, ces dix dernières années sont aussi profondément marqués par une médiatisation croissante du cyberterrorisme. La propagande de l'État Islamique n'a pas manqué de faire parler d'elle dans les médias. Le cyberterrorisme change le territoire habituel de la guerre, qui quitte la matérialité du territoire pour investir des mondes virtuels. La victoire par la force n'est plus une obligation car un individu seul peut maintenant prétendre s'attaquer à de grandes organisations (Arpagian, 2018).

Jarno Limnéll affirme que la « cyber-guerre » débutera dans un futur proche (Limnéll, 2013). Les gouvernements sont en plein développement de leurs infrastructures consacrées au cyberespace. Le principal motif exposé publiquement est la sécurité nationale : elle recouvre la défense des organismes publics et privés vitaux aux nations. Ces infrastructures essentielles reposent partiellement ou totalement sur le numérique : les centrales nucléaires, les centrales électriques, les fichiers publics nationaux, les réseaux de transport, ... À l'inverse de cette motivation, des cyberattaques entre états sont relevés à plusieurs niveaux.[39] L'auteur convoque des éléments qui prédisposent les prochaines années à un nombre de cyberattaques toujours plus croissant. Les coûts de la « cyber-guerre » sont bien moins élevés que dans une guerre classique tout en assurant des dégâts considérables, l'origine des attaques est plus propice à l'anonymat et le cyberespace rend l'attaque aisée par rapport à la défense (Limnéll, 2013 : 34). En mai 2018, le président français Emmanuel Macron a rencontré son homologue russe Vladimir Poutine à Saint Pétersbourg, le sujet des cyberattaques a été abordé en conférence de presse.[40] Les deux représentants ont dialogué des cyberattaques entre nations sans remettre en cause leurs existences et ont évoqué l'importance de suivre des règles communes sur le cyberespace.

Officiellement, les forces militaires françaises se voient munir d'unités spécialisées dans la gestion et la lutte contre la cybercriminalité et ses actes (*cf.* Figure 16). Nous sommes typiquement face à des cyber-guerriers étatiques si l'on en suit le raisonnement de Daniel

[39] https://www.lemonde.fr/pixels/article/2018/10/04/les-occidentaux-se-coordonnent-pour-accuser-la-russie-de-cyberattaques_5364802_4408996.html
[40] https://www.youtube.com/watch?v=WJGKuspi0-Q

Ventre (Ventre, 2012). Nous nous permettons de faire un lien avec les propos recueillis lors des entretiens (*cf.* Annexe 15).

Figure 16 : 807e compagnie de transmissions (8e CTRS) (Source : Ouest-France[41])

Malgré le faible volume de recherches sur la notion de « cyber-guerrier », des premiers travaux émergent progressivement. Les domaines de recherche sur la sécurité et la défense sont des précurseurs sur ces questions, ils nous décrivent déjà des liens étroits avec le milieu cybercriminel en plus de reconnaitre ce nouveau terme de « cyber-guerrier » comme véritable objet soumis à représentation.

[41] https://www.ouest-france.fr/bretagne/ille-et-vilaine/la-807-l-unite-bretonne-des-cybersoldats-5646237

Conclusion

Tout au long de ce travail de recherche, nous nous sommes interrogés sur les imaginaires, nous avons tenté de comprendre comment se construit une représentation et nous avons mesuré son influence sur les individus. Depuis les données que nous avons pris soin de récolter auprès d'œuvres accessibles à tous et de témoignages, nous apportons modestement notre regard sur la base des connaissances scientifiques qui traitent du sujet. Les représentations du cybercriminel développées dans les œuvres culturelles ont un impact fort sur l'imaginaire collectif et tendent à homogénéiser les perceptions et les stéréotypes. Du côté des professionnels du numérique, la représentation du cybercriminel varie en fonction de la profession occupée et de l'expérience. Il n'y a pas une unique représentation du cybercriminel mais bel et bien une multitude, certaines ayant une plus forte influence que d'autres. Cette figure du numérique a évolué dans le temps et sera encore amenée à se modifier ; elle se situe au cœur des enjeux numériques de demain. Il est certain que d'autres représentations numériques apparaîtront dans les prochaines années en plus de celles qui existent déjà. En nous posant les bons questionnements à leurs égards, nous pourrons encore mieux saisir toute la complexité du cyberespace et ses effets sur nos vies.

À l'issue de ce travail, nous avons comme principal regret de n'avoir trouvé qu'assez tardivement une thèse datant de 2007 portant sur les images sociales du pirate informatique soutenue par Jean-Philippe Humbert sous la direction de Jacques Walter à l'Université de Lorraine : thèse qui nous aurait été très utile durant la première partie de ce travail. Un autre travail, publié en mars 2020, « Les imaginaires de l'informatique à travers quelques 'figures' marquantes : bricoleur, pirate, hacker… » au plus proche de nos intérêts n'a été ainsi lu qu'au moment du dépôt de ce travail alors qu'il aurait pu participer grandement à notre réflexion, notamment du point de vue méthodologique.

Similairement à d'autres travaux scientifiques, nous aurions souhaité plus de réponses au questionnaire mais il en va ainsi, cela fait pleinement partie de la recherche que d'aller chercher des données parfois plus ou moins accessibles, le contexte influant également. Nous remercions toutes les personnes qui se sont prêtées à l'exercice, aussi bien au travers du formulaire que dans les entretiens en visioconférence ; nul ne doute que ces témoignages constituent et resteront une base de données pertinente, bénéfique pour aujourd'hui et à l'avenir.

En points positifs de ces recherches, nous retiendrons un état de l'art argumenté et détaillé grâce à de nombreuses lectures et à des travaux scientifiques d'une grande qualité fournis par des

chercheurs de différentes disciplines. Nous soulignons aussi un corpus d'œuvres culturelles riche en informations sur le cybercriminel, toujours perfectible certes, mais qui a le mérite d'exister à ce jour et de servir. Nous espérons avoir amené des connaissances, un savoir et une réelle réflexion autour de cet objet d'étude qu'est la représentation du cybercriminel avec ce travail.

Personnellement, cet exercice m'a énormément appris sur moi-même et sur le sujet de mes recherches. J'ai pu me cultiver et m'essayer à une démarche scientifique rigoureuse. L'expertise acquise tout au long ce travail m'est très chère pour mon avenir professionnel. Elle me permet d'ajouter un regard critique, une observation, une analyse sur la mise en place de dispositifs numériques conformément à une logique de cybersécurité, de connaissances sur les potentielles attaques et de savoirs sur les auteurs de ses attaques. Des points qui sont particulièrement ancrés avec ma formation en Master Création de Projets Numériques à l'UFR SHS de Metz. En outre, cette expérience acquise me permet de sensibiliser sur la déconstruction de préjugés et de symboles forts liés à la cybercriminalité et d'informer sur certains bons gestes à adopter.

Si nous devions envisager les perspectives futures de ce travail, nous pourrions nous pencher sur d'autres figures numériques fortes qui ont émergé avec les TIC et étudier en quoi celles-ci diffèrent ou non de notre travail sur le cybercriminel (quels mécanismes, …). Par ailleurs, il serait aussi intéressant d'amener plus loin la dimension professionnelle en recueillant davantage de témoignages sur la durée ainsi que dans d'autres secteurs d'activité.

Bibliographie

Arpagian, N. (2018). *La cybersécurité*. Paris cedex 14, France: Presses Universitaires de France.

Barthes, R. (1957). *Mythologies.* Paris, France: Éditions du Seuil.

Benbouzid, B. & Ventre, D. (2016). « Pour une sociologie du crime en ligne: Hackers malveillants, cybervictimations, traces du web et reconfigurations du *policing* ». *Réseaux*, 197-198(3), 9-30. doi:10.3917/res.197.0009.

Bertin, G., Bigay, R., Doutreix, M., Jeannerod, M. & Papastamkou, S. (2020). « Les imaginaires de l'informatique à travers quelques 'figures' marquantes : Bricoleur, pirate, hacker… » [Billet]. *Carnet de recherche de l'Inathèque*. Consulté 18 juin 2020, à l'adresse https://inatheque.hypotheses.org/20467

Cardon, D. (2010). *La Démocratie Internet*. Paris, France : Éditions du Seuil.

Casilli, A. (2011). « Trois idées reçues sur Internet ». *Sciences Humaines*, 229(9), 11-11.

Casilli, A. (2015). « Dr Popp et la disquette Sida. Sociologie d'une affaire hacker ». *Terrain. Anthropologie & sciences humaines*, (64), 14-31.

Coleman, G., & Calvé, N. (2016). *Anonymous : Espions, hackers, lanceurs d'alertes...* LUX EDITIONS.

Côté, A., Bérubé, M. & Dupont, B. (2016). « Statistiques et menaces numériques: Comment les organisations de sécurité quantifient la cybercriminalité ». *Réseaux*, 197-198(3), 203-224. doi:10.3917/res.197.0203.

Dagiral, É. (2008). « Pirates, hackers, hacktivistes : déplacements et dilution de la frontière électronique ». *Critique*, 733-734(6), 480-495. doi:10.3917/criti.733.0480.

Danic, I. (2006). « La notion de représentation pour les sociologues ». Premier aperçu. *ESO*, (25), 29-32.

Dupont, B., & Gautrais, V. (2010). « Crime 2.0 : Le web dans tous ses états ! » *Champ pénal/Penal field*, (Vol. VII). Consulté à l'adresse http://journals.openedition.org.bases-doc.univ-lorraine.fr/champpenal/7782

Dupont, B. (2014). « La régulation du cybercrime comme alternative à la judiciarisation : le cas des botnets ». *Criminologie*, 47 (2), 179–201. https://doi.org/10.7202/1026733ar

Flichy, P. (2001). 4. « Du mythe d'Internet au cyber-imaginaire ». Dans : P. Flichy, *L'imaginaire d'Internet* (pp. 113-134). Paris: La Découverte.

Ghernaouti, S. & Dufour, A. (2017). « Chapitre V - Cybercriminalité et cybersécurité ». Dans : Solange Ghernaouti éd., Internet (pp. 101-118). Paris cedex 14, France: Presses Universitaires de France.

Grabosky P. N. (2001). "Virtual criminality: old wine in new bottles". *Social & Legal Studi*es, 10(2), 243-249.

Guarnieri, F. & Przyswa, É. (2012). « Cybercriminalité et contrefaçon : pour une nouvelle analyse des risques et des frontières ». *Hermès*, La Revue, 63(2), 175-180. https://www.cairn.info/revue-hermes-la-revue-2012-2-page-175.htm.

Lang, F. (2008). « L'identification de l'auteur de contenus illicites et des intermédiaires techniques : le constat ». *LEGICOM*, 41(1), 39-41. doi:10.3917/legi.041.0039.

Leman-Langlois, S. (2006). « Questions au sujet de la cybercriminalité, le crime comme moyen de contrôle du cyberespace commercial ». *Criminologie*, 39 (1), 63–81. https://doi.org/10.7202/013126ar

Limnéll, J. (2013). « Le cyber change-t-il l'art de la guerre ? ». *Sécurité globale*, 23(1), 33-41. doi:10.3917/secug.023.0033.

Ouimet, M. (2006). « Réflexions sur Internet et les tendances de la criminalité ». *Criminologie*, *39* (1), 7–21. https://doi.org/10.7202/013123a

Pansier, F. & Jez, E. (2000). *La criminalité sur l'Internet.* Paris cedex 14, France: Presses Universitaires de France.

Paquot, T. (2019). « Le cinéma, petite fabrique de stéréotypes ». *Hermès*, La Revue, 83(1), 119-124. https://www.cairn.info/revue-hermes-la-revue-2019-1-page-119.htm.

Ventre, D. (2012). « Le cyber-guerrier : nouvelle figure combattante au service de la cyber-défense ». *Sécurité et stratégie*, 11(4), 39-48. doi:10.3917/sestr.011.0039.

Wall D. S. (2015). “Dis-Organised Crime: Towards a Distributed Model of the Organization of Cybercrime”. *The European Review of Organised Crime*, 2(2), 71-90.

Glossaire

Analyseur de paquets : logiciel qui permet d'intercepter les communications (chiffrées ou non chiffrées) entre un réseau et un système informatique (ex : Wireshark, …).

Attaque par dictionnaire : elle est similaire à l'attaque par force but puisqu'elle vise également à dérober un mot de passe ou une clé. Elle se base sur une liste de mots, de mots de passe couramment utilisés ou récemment dérobés.

Attaque par force brute : fait de tester par la puissance de calcul d'un système informatique toutes les combinaisons possibles pour trouver un mot de passe, une clé. Les combinaisons sont entrées automatiquement les unes après les autres.

***Backdoor* :** porte d'entrée cachée à l'utilisateur légitime au sein d'un programme. Elle permet à un autre utilisateur potentiellement malveillant de se connecter à la machine pour y exécuter de multiples actions.

Carding : trafic de cartes de crédit, de coordonnées bancaires par internet. Cela regroupe également d'autres pratiques en lien.

Cloud : abrégé de *Cloud Computing* qui désigne l'informatique « en nuage ». Le Cloud est l'appel d'informations à des serveurs multiples distants.

***Dark Web* :** « partie sombre d'internet », c'est une partie d'Internet n'utilisant pas les protocoles habituels d'Internet rendant spécifiquement opaques les adresses IP des individus s'y connectant. Des sites Web, des solutions logicielles et une grande quantité de contenus en tout genre non référencée par les moteurs de recherche classiques y sont présents. Le *Dark Web* est principalement connu pour être un des lieux de référence en matière de cybercriminalité bien qu'elle n'y est pas majoritaire en comparaison à tous les autres contenus présents.

Enregistreur de frappe *(Keylogger)* : un enregistreur de frappe est un logiciel espion qui enregistre les touches saisies au clavier. Il peut être directement sous forme numérique ou s'établir depuis un périphérique comme une clé USB.

***Fandom* :** communauté regroupant les fans d'une œuvre, d'un domaine. Les *fandom*s sont par ailleurs présents sous forme semblable à des Wikis sur Internet.

Hameçonnage (*Phishing*) : fait de se faire passer pour une organisation de confiance (par l'intermédiaire d'un site, d'un mail, …) dans l'objectif de récolter des données personnelles.

Ingénierie sociale : fait de manipuler psychologiquement un ou des individus à des fins malveillantes.

Piratage téléphonique (*Phreaking*) : ce sont toutes les pratiques relatives au piratage téléphonique.

Rançongiciel/*Ransomware* : logiciel malveillant qui bloque l'accès à un système informatique en cryptant tout ou une partie des données de celui-ci. Il demande ensuite une rançon afin de permettre à l'utilisateur légitime de récupérer ou non ses données.

Rootkit : logiciel malveillant qui pénètre d'autres logiciels ou d'autres ressources numériques pour échapper à toute détection du support informatique hôte. Il peut proposer une multitude d'outils cybercriminels.

Scanner de ports : logiciel qui va envoyer des requêtes à un système informatique afin de récolter des données sur celui-ci dans le but de savoir spécifiquement quels ports sont ouverts ou non (ex : Nmap, …).

Ubérisation : remise en cause du modèle économique d'une entreprise ou d'un secteur d'activité par l'arrivée d'un nouvel acteur proposant les mêmes services à des prix moindres, effectués par des indépendants plutôt que des salariés, le plus souvent via des plateformes de réservation sur Internet (Source : *Dictionnaire Larousse*).

Ver informatique : logiciel malveillant qui a la faculté de se diffuser sur d'autres systèmes informatiques par le biais d'un réseau.

Virus : un logiciel malveillant qui a pour but d'endommager un système informatique.

Annexes

Pour des raisons de praticité et de lisibilité, certaines annexes sont jointes numériquement.

Annexe 13 : lien d'accès à la grille d'analyse complète du corpus d'œuvres culturelles (format tableur)

- https://tinyurl.com/y93evpug

Annexe 14 : lien d'accès au formulaire / questions des entretiens menés (Google Forms)

- https://tinyurl.com/ydgobppe

Annexe 15 : lien d'accès à l'entretien 1 avec M. Franck Bettanier (format vidéo)

- https://tinyurl.com/ya8nu57d

Annexe 16 : lien d'accès à l'entretien 2 avec M. Nicolas Chevrier (format vidéo)

- https://tinyurl.com/y8foqwwn

Annexe 17 : lien d'accès aux réponses du formulaire (Google Sheets)

- https://tinyurl.com/y72usamt

Annexe 18 : lien d'accès à la retranscription de l'entretien 1 avec M. Franck Bettanier

- https://tinyurl.com/y8gnwhck

Annexe 19 : lien d'accès à la retranscription de l'entretien 2 avec M. Nicolas Chevrier

- https://tinyurl.com/yc3tww7d

Sexe du cybercriminel représenté	Effectifs	Pourcentages
H	57	81%
F	11	16%
ND	2	3%
TOTAL	70	100%

Annexe 1 : sexe du cybercriminel représenté dans les œuvres culturelles analysées (H/F)

Réalisateur(rice) de l'œuvre	Effectifs	Pourcentages
H	66	94%
F	4	6%
ND	0	0%
TOTAL	70	100%

Annexe 2 : sexe du réalisateur(rice) des œuvres culturelles analysées (H/F)

Cybercriminel(s) dans l'œuvre	Effectifs	Pourcentages
U	30	43%
M	39	56%
ND	1	1%
TOTAL	70	100%

Annexe 3 : présence Unique ou Multiple de cybercriminel(s) dans les œuvres culturelles analysées (U/M)

Tranche d'âge du cybercriminel représenté	Effectifs	Pourcentages
0-15	1	1%
15-25	25	36%
25-50	40	57%
50 et +	0	0%
ND	4	6%
TOTAL	70	100%

Annexe 4 : tranche d'âge du cybercriminel représenté dans les œuvres culturelles analysées

Lien de la profession du cybercriminel représenté avec le numérique	Effectifs	Pourcentages
Liée au numérique	26	37%
Non liée au numérique	6	9%
Non concernée	35	50%
ND	3	4%
TOTAL	70	100%

Annexe 5 : lien de la profession du cybercriminel représenté avec le numérique dans les œuvres culturelles analysées

CSP du cybercriminel représenté	Effectifs	Pourcentages
Artisans, commerçants et chefs d'entreprise	10	14%
Cadres et professions intellectuelles supérieures	6	9%
Professions intermédiaires	14	20%
Ouvriers	1	1%
Employés	1	1%
Autres personnes sans activité professionnelle	35	50%
ND	3	4%
TOTAL	70	100%

Annexe 6 : catégorie socioprofessionnelle du cybercriminel représenté dans les œuvres culturelles analysées

Actes du cybercriminel représenté	Effectifs	Pourcentages
Vol de données	57	23%
Falsification de données	12	5%
Suppression de données	8	3%
Détournement de caméra(s)de vidéosurveillance	20	8%
Détournement de webcam(s)	11	5%
Usurpation d'identité	8	3%
Ingénierie sociale	7	3%
Phishing	4	2%
Carding	4	2%
Phreaking	8	3%
Cyberharcèlement	5	2%
Création de logiciel(s) malveillant(s)	18	7%
Détournements de fonds	17	7%
Détournement de services publics (circulation routière, électricité, …)	2	1%
Détournement de satellite(s)	7	3%
Commerce illégal	5	2%
Prise de contrôle en temps réel de système informatique à distance	23	9%
Attaque par dictionnaire	2	1%
Attaque par force brute	3	1%
Usage de ver informatique	1	0%
Usage de botnets	1	0%
Usage d'un enregistreur de frappe	1	0%
Usage de rootkit	1	0%
Usage de backdoor	3	1%
Spam	1	0%
Géolocalisation de système(s) informatique(s)	9	4%
Détournement d'un système domotique / Déverrouillage de portes sécurisées	5	2%
TOTAL	243	100%

Annexe 7 : actes du cybercriminel représenté dans les œuvres culturelles analysées

Lien social du cybercriminel représenté	Effectifs	Pourcentages
Famille	0	0%
Virtuel	0	0%
Réel	28	40%
Famille et réel	9	13%
Famille et virtuel	1	1%
Virtuel et réel	19	27%
Famille, virtuel et réel	4	6%
Aucun	6	9%
ND	3	4%
TOTAL	70	100%

Annexe 8 : lien social du cybercriminel représenté dans les œuvres culturelles analysées

Style vestimentaire / Apparence physique du cybercriminel représenté	Effectifs	Pourcentages
Soigné	13	19%
Correct	46	66%
Atypique	7	10%
ND	4	6%
TOTAL	70	100%

Annexe 9 : style vestimentaire / apparence physique du cybercriminel représenté dans les œuvres culturelles analysées

La représentation du cybercriminel - TER - Master CPN - MORES Quentin

Ce questionnaire intervient dans le cadre du mémoire de recherche de M. Quentin MORES, étudiant en Master Création de Projets Numériques (CPN) à l'Université de Lorraine pour l'année 2019/2020. Ce travail porte sur la représentation du cybercriminel. Ce questionnaire s'adresse donc aux professionnels du numérique et ne vous prendra pas plus de 15 à 20 minutes.

Par ce travail, nous cherchons à comprendre comment s'est construite la représentation de la figure du cybercriminel, principalement à partir des œuvres culturelles (films, séries, ...), mais également à qualifier la représentation qu'en ont les professionnels, à partir des imaginaires ou du terrain.

Pensez à bien valider le questionnaire avant de quitter.

Pouvez-vous décrire rapidement votre parcours de formation ?

Votre réponse

Quelles sont aujourd'hui vos responsabilités ?

Votre réponse

Comment définiriez-vous la cybercriminalité ?

Votre réponse

Faites-vous des distinctions entre "hacker", "cybercriminel", "pirate" ou tout autre terme que vous utilisez ?

Votre réponse

Quels sont les actes malveillants auxquels ils peuvent se livrer le plus fréquemment?

- [ ] Vol de données
- [ ] Falsification de données
- [ ] Suppression de données
- [ ] Détournement de caméra(s) de vidéosurveillance
- [ ] Détournement de webcam(s)
- [ ] Usurpation d'identité
- [ ] Ingénierie sociale
- [ ] Phishing
- [ ] Carding
- [ ] Phreaking
- [ ] Cyberharcèlement
- [ ] Création de logiciel(s) malveillant(s)
- [ ] Détournements de fonds
- [ ] Détournements de services publics (circulation routière, électricité, ...)
- [ ] Détournement de satellite(s)
- [ ] Commerce illégal
- [ ] Prise de contrôle en temps réel d'un système informatique à distance
- [ ] Attaque par dictionnaire
- [ ] Attaque par force brute
- [ ] Usage de ver informatique
- [ ] Usage de botnets
- [ ] Usage d'un enregistreur de frappe
- [ ] Usage de rootkit
- [ ] Usage de backdoor
- [ ] Spam
- [ ] Géolocalisation de système(s) informatique(s)
- [ ] Détournement d'un système domotique/Déverrouillage de portes sécurisées
- [ ] Autre : _____

Annexe 10 : formulaire / questions des entretiens menés (partie 1)

Partie 2/3

Pourriez-vous dire si cette représentation a été influencée par des films, des romans, des séries... Et si oui, quelles sont les œuvres qui vous ont le plus influencé ?

Votre réponse

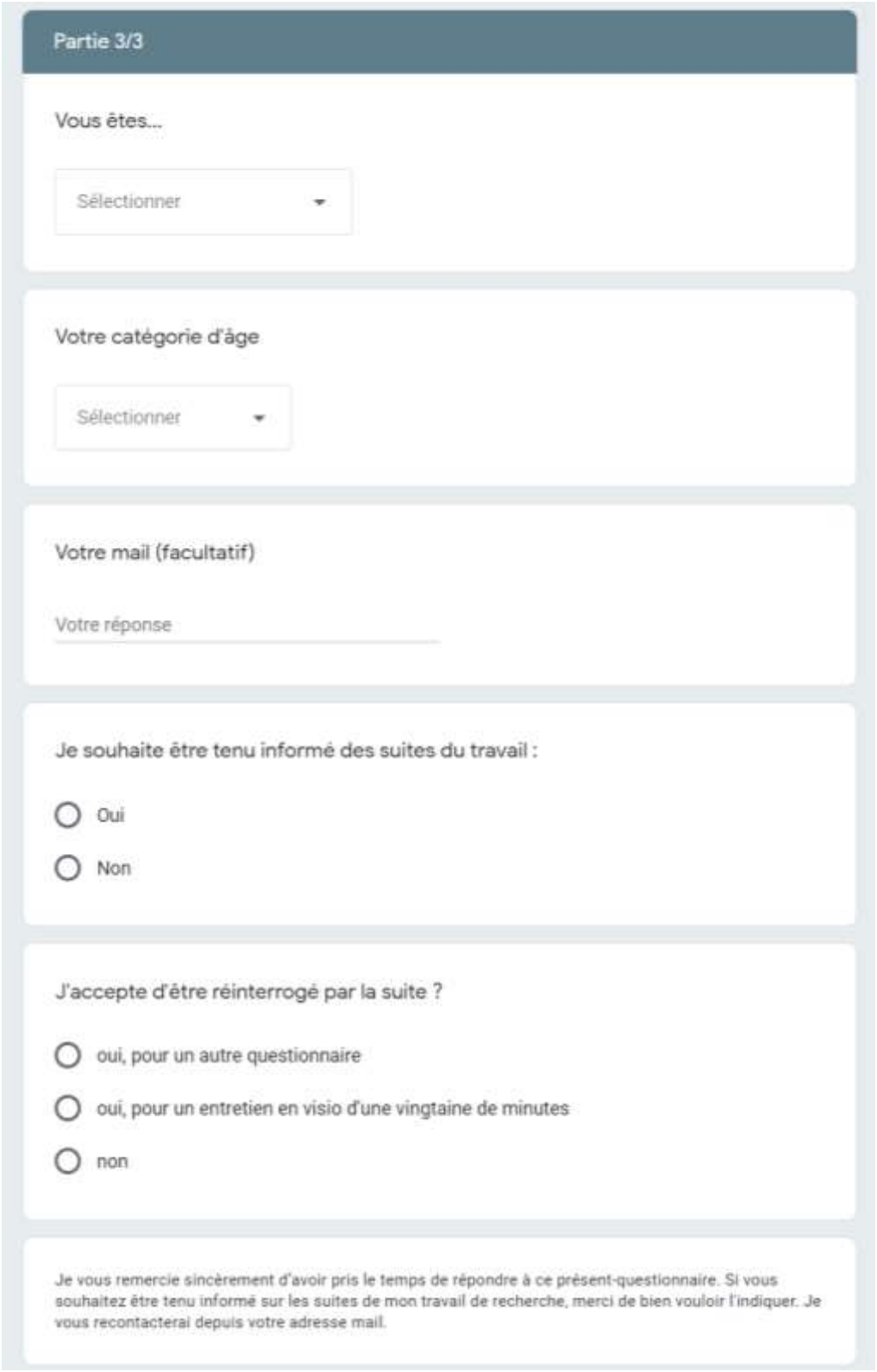
Votre travail de terrain a-t-il modifié cette représentation ?

- ☐ Oui
- ☐ Non
- ☐ Sans opinion

Pour chacune de ces affirmations, choisissez votre posture.

	Tout à fait d'accord	Plutôt d'accord	Plutôt pas d'accord	Pas du tout d'accord	Sans opinion
Il y a un profil type du cybercriminel	☐	☐	☐	☐	☐
Il y a souvent des traits communs chez les cybercriminels	☐	☐	☐	☐	☐
Il y a des traits communs dans les parcours de vie	☐	☐	☐	☐	☐
il y a des traits communs dans la psychologie	☐	☐	☐	☐	☐
Je pense qu'il y a une grande hétérogénéité de profils chez les cybercriminels	☐	☐	☐	☐	☐

Annexe 11 : formulaire / questions des entretiens menés (partie 2)



Annexe 12 : formulaire / questions des entretiens menés (partie 3)

Table des figures et tableaux

Quentin Mores

quentin.mores1@etu.univ-lorraine.fr

Sous la direction de Marie Chagnoux : marie.chagnoux@univ-lorraine.fr

La représentation du cybercriminel – Des imaginaires socio-culturels aux réalités professionnelles

Encore peu médiatisée il y a une dizaine d'années, la cybercriminalité est devenue un enjeu de taille pour toutes les institutions qu'elles soient étatiques ou commerciales en même temps qu'elle devenait un sujet de plus en plus diffusé pour le grand public. Par ce travail, nous cherchons à comprendre comment s'est construite la représentation de la figure du cybercriminel, principalement à partir des œuvres culturelles (films, séries, ...) et à confronter cet imaginaire aux représentations qu'en ont les professionnels, à partir de ces imaginaires en tension avec leur expérience du terrain.

Mots clés : *cybercriminalité, cybersécurité, hameçonnage, hack, logiciel rançonneur, sécurité informatique, cyberviolence, représentation mentale, représentation sociale.*

The representation of the cybercriminal - From socio-cultural imaginations to professional realities

Cybercrime, which was not widely publicised about ten years ago, has become a major issue for all institutions, whether state or commercial, at the same time as it has become an increasingly popular subject. Through this work, we seek to understand how the representation of the figure of the cybercriminal was constructed, mainly from cultural works (films, series ...) and to confront this imaginary with the representations that the professionals have, from these imaginations in tension with their experience of the field.

Key words : *cybercrime, cybersecurity, phishing, hack, ransomware, computer security, cyberviolence, mental representation, social representation.*