Travail de fin d'études[BR]- Travail de fin d'études: ""Access Granted" : étude sur les motivations des hackers à se tourner vers la légalité et pertinence du hacking légal comme vecteur de désistance."[BR]- Séminaire d'accompagnement à l'écriture

Auteur : Collard, Nicolas
Promoteur(s) : Dantinne, Michaël
Faculté : Faculté de Droit, de Science Politique et de Criminologie
Diplôme : Master en criminologie à finalité spécialisée en organisations criminelles et analyse du crime
Année académique : 2023-2024
URI/URL : http://hdl.handle.net/2268.2/21909

COLLARD Nicolas

Travail de fin d'études en vue de l'obtention du Master en Criminologie, en finalité spécialisée en organisations criminelles et en analyse du crime

Année académique 2023-2024

« Access Granted » : étude sur les motivations des hackers à se tourner vers la légalité et pertinence du hacking légal comme vecteur de désistance

LIÈGE université
Droit, Science Politique & Criminologie

Recherche menée sous la supervision de
Monsieur Michaël Dantinne,
Professeur à l'Université de Liège.

Remerciements

Je tiens premièrement à remercier le professeur Michaël Dantinne de m'avoir fait confiance avec cette proposition de T.F.E., de m'avoir permis d'agir en autonomie tout au long de ce travail mais de s'être rendu disponible quand j'en faisais la demande.

Je tiens aussi à remercier tous les participants qui ont accepté de me rencontrer pour me faire part de leur expérience.

Je remercie également les professeures Vanessa Franssen et Cécile Mathys qui, au cours de conversations de couloir, ont pu me prodiguer des conseils précieux quant à la bonne réalisation de ce travail et de m'avoir parfois aiguillé vers des solutions que je n'avais pas prises en compte.

Finalement, j'aimerais remercier mes 2 relecteurs pour m'avoir apporté un dernier feedback et pour m'avoir apporté leur point de vue externe ainsi que toute personne qui a participé de près ou de loin à la réalisation de cet écrit.

Table des matières

Abstract

La technologie ne cesse de prendre de plus en plus de place dans notre société et, avec elle, ses dangers intrinsèques. Or, peu de recherches s'intéressent à ceux qui ont permis cette évolution ou la protection contre les abus, les hackers. L'objectif de cette recherche est donc de rendre compte des différentes motivations animant des hackers repentis à s'être tournés vers la légalité et à l'impact qu'un métier légal dans le domaine a pu avoir sur leur désistance. L'échantillon est composé de 5 hommes recrutés par l'intermédiaire du Centre Cybersécurité Belgique ou ayant répondu à un appel sur les réseaux sociaux. Ils sont rencontrés au travers d'entretiens semi-directifs par visioconférence ou par mail, dans une méthodologie qualitative. Les résultats indiquent que les motivations au moment de se lancer dans le hacking sont principalement les mêmes qu'après en avoir fait son métier, avec l'arrivée d'une volonté de protéger les systèmes informatiques et d'avoir un impact bénéfique sur la société. Ils montrent aussi que le métier n'arrive qu'après une désistance aboutie et n'a donc pas d'effet dessus, laissant plutôt la place à des explications liées à la maturation ou à des facteurs sociaux. Ces observations permettent de questionner les problématiques liées à l'étude de ce domaine, d'orienter les futures recherches et de dégager quelques pistes de réflexion sur les réactions et adaptations possibles tant au niveau législatif qu'au niveau sociétal.

Mots-clefs : hacking légal/éthique – désistance/désistement – motivations – qualitatif

---

Technology is becoming more and more important in our society and, with it, its intrinsic dangers. However, few studies have shown interest towards those who made this evolution and the protection against possible abuse, hackers. The objective of this study is to examine the motivations that had reformed hackers turn to legality and how a legal job in the field may have impacted their desistance. The sample consists of 5 men recruited through the Cybersecurity Centre in Belgium or by responding to a call on social networks. They are met through semi-structured interviews either given by mail or through videoconference, in a qualitative methodology. Results show that motivations for engaging in hacking stay the same after getting employed, with the arrival of a desire to protect information systems and to have a beneficial impact on the society. It also shows that getting a job only occurs after a successful desistance and, hence, has no effect on it, leaving room instead on elements linked to maturation or social factors. These observations make it possible to question of issues related to this field of research, to guide future research and to identify some avenues of reflexion for possible answers and adaptations at both the legislative and at the societal levels.

Keywords: legal/ethical hacking – desistance – motivations - qualitative

Introduction

1. Intérêt de l'étude

La technologie prend une place de plus en plus grande dans notre société et, comme l'observaient déjà Peter N. Grabosky, Russell, G., Smith & Paul Wright en 1998, le développement de la technologie, s'il nous offre des opportunités incroyables, est inévitablement accompagné de risques sous la forme d'opportunités criminelles. Malgré les années, le même constat est fait par de nombreux auteurs (Holt, T. J., 2020 ; Oreku, G. S. & Mtenzi F. J., 2017 ; Gillespie, A. A., 2019 ; Choi, K.S., Lee, C.S., Louderback, E.R., 2020 ; Furnell, S., 2002 ; Yar, M. & Steinmetz, K. F., 2019 ; Noordegraaf, J. E. & Kranenbarg, M. W., 2023 ; …). Marleen Weulen Kranenbarg (2019) va jusqu'à dire que la distinction communément faite entre infractions cyber-dépendantes (hacking, Distributed Denial of Services, Ransomware, ...) et infractions cyber-facilitées (fraudes, contrefaçons, …) continuera de se réduire à mesure que la société se numérisera jusqu'à ce qu'elles se confondent. Ainsi, il n'est pas étonnant aujourd'hui encore, de voir de nombreux auteurs s'intéresser aux risques liés aux nouvelles technologies, notamment avec l'émergence de l'intelligence artificielle (Bikeev, I. I. & al., 2019 ; Blauth, T. F., Gstrein, O. J. & Zwitter, A., 2022 ; Hayward, K. J. & Maas, M. M., 2021 ; Mahmud, A., 2023 ; …). Un rapport des tendances criminelles dans le monde rendu par Interpol en 2022 (Interpol, 2022) appuie sur le fait que la cybercriminalité constitue une des 5 tendances qui représentent le plus gros risque au niveau mondial, et mettent en avant une attention particulière aux actes de phishing (« *un acte évolutif de tromperie où l'auteur se fait passer pour un autre afin d'obtenir des informations sur sa cible* » - E.E. Lastdrager 2014), de ransomware (« *acte de monétisation illégale d'informations auxquelles un auteur a accédé illégalement, contre la récupération desquelles la cible devra payer une rançon* » - Paquet-Clouston, M. & al. – 2019), de fraudes en ligne et d'intrusion informatique. Finalement, une analyse de Statista de novembre 2022 prévoit que le coût associé aux entreprises victimes de cybercriminalité pourrait grimper à 23.82 billions de dollars, ce qui correspond presque au triple du coût actuel estimé de 8.44 billions de dollars. Finalement, au vu des caractéristiques propres à la cybercriminalité, Steven Furnell (2002) estime que seulement 5% des infractions cybercriminelles sont reportées aux autorités, constat sur lequel s'appuient Majid Yar & Kevin F. Steinmetz (2019) pour dire « les problèmes posés par la cybercriminalité pourraient bien figurer dans les plus urgents [à traiter] du début du 21ème siècle »[1]. Il semble, en ce sens, nécessaire que davantage de littérature doive être créée afin d'informer sur ces risques mais aussi sur les solutions qui peuvent être données en réponse à la cybercriminalité.

Une raison qui pousse à penser que cette étude spécifiquement est résolument pertinente est la réponse qu'elle apporte à deux manques présents dans la littérature actuelle : le premier est la rareté d'études ayant pour objectif d'informer sur la désistance du hacking. Une revue systématique de littérature de Joeri Loggen, Asier Moneva & Rutger Leukfeldt de 2023 indique que seulement 14 articles étaient disponibles (du moins, en anglais) sur ce sujet. A ce niveau, une étude de Mario Silic & Paul Benjamin Lowry (2019) qui étudient la façon dont un échantillon de *black hat* hackers parvient à gérer le stress lié à cette activité, appuie sur la perspective de recherches futures qui s'intéresseraient à un panel d'ex-hackers illégaux et aux motivations qui les ont poussés à se tourner vers le hacking légal. Le second est l'absence de recherches sur le hacking dit « éthique »[2], les multiples articles ont plutôt tendance à décrire les activités qui y sont liées sans vraiment aller étudier le hacker en lui-même (Brown, C., 2015 ; Chang, L. YC. & Whitehead, J., 2021 ; Nicholson, S., 2019 ; Zand, E. & al., 2021), ou ses motivations à devenir ou à rester hacker « éthique ». Une exception notable à ce constat est l'article de Judith E. Noordegraaf & Marleen Weunen Kranenbarg (2023) qui étudie les motivations d'individus à s'être tournés vers le

[1] Traduction personnelle des termes utilisés par Yar, M. & Steinmetz, K.F., 2019. Cybercrime and Society. P.45. : « {Moreover, if we bear in mind estimates that as little as 5 per cent of such crimes may actually be reported to the authorities (Furnell, 2002: 190),} then the problems posed by cybercrime may well figure among the most urgent of the early twenty-first century. »

[2] Cette notion sera débattue dans le titre 2.1.3.

hacking « éthique » avant l'âge de 18 ans et à l'être restés au fil des années. La volonté de cette présente recherche était alors de combler ces 2 manques en s'intéressant au lien qui unit la désistance et le hacking légal.

2. Concepts abordés

2.1. Le hacking

Le hacking est défini par Peter N. Grabosky (1998) comme « *une intrusion dans un système informatique avec une intention criminelle* »[3]. Et nombreux auteurs continuent aujourd'hui d'appliquer cette définition (Maimon, D. & Louderback, E. R., 2019 ; Jordan, T. & Taylor, P., 1998 ; Chang, L-Y. C. & Whitehead, J., 2021 ; …). Cette définition semble montrer que le concept de hacking est relativement mal compris et appliqué de façon réductrice à un comportement porté par l'illégalité qui le caractérise. Il est alors important de faire un détour par la définition du hacking comme entendu dans cette recherche. Pour ce faire, un brin d'histoire sera abordé pour comprendre l'évolution de la perception du hacking. Il sera ensuite fait état de plusieurs typologies communes de hackers et, finalement, du choix de la terminologie employée dans cette étude afin de garantir que le lecteur ait en sa possession toute information nécessaire à la bonne compréhension de cet article.

2.1.1. Une brève histoire du hacking

Les premiers comportements reliés à du « hacking » apparaissent dans le début des années '40 dans l'Institut Technologique du Massachusetts (M.I.T.). En réalité, à cette époque, les ordinateurs sont encombrants et les programmes extrêmement lents à exécuter, c'est pourquoi certains « programmeurs » décident de manipuler les circuits électriques du système pour en accélérer les processus. A ce moment, le « hacking » tire surtout son nom du verbe « to hack » en anglais qui signifie « couper ». Ce terme rapporte originellement au fait de raccourcir et donc, de couper, les temps d'exécution des ordinateurs. A cette époque, le concept a alors une connotation, si pas positive, au moins neutre au sein de la société. (Levy, S., 2010; Steinmetz, K. F., 2015; Turkle, S., 1984)

L'arrivée de la perception du hacking comme étant illégal survient dans les années '60 lorsque John Draper, alias « Captain Crunch » a l'idée d'utiliser un sifflet trouvé comme cadeau dans un paquet de céréales pour intercepter des appels longue distance de la compagnie téléphonique « AT&T », évitant ainsi les frais qui y sont généralement associés (Furnell, S. 2002). Cet acte sera nommé le « phreaking » et est généralement reconnu comme étant à l'origine du « hacking ». (DeJarvis, O. & Randolph, A. B., 2022)

Les prochaines années seront révolutionnaires d'un point de vue technologique : d'abord, la fin des années '60 voit apparaitre ce qu'on appelle « ARPANET », la première mise en réseau de plusieurs ordinateurs entre eux, qui mènera, plus tard, à la création de l'Internet moderne. D'autre part, les ordinateurs se font plus petits et moins chers, ce qui provoque l'apparition des premiers ordinateurs domestiques. Ces deux innovations mènent assez rapidement, dans les années '70, à la création des premiers « forums » appelés *Bulletin Board Systems*, c'est par cet intermédiaire, ainsi que par divers magazines papier, que se développera une sous-culture du hacking : les techniques et les pratiques sont partagées beaucoup plus simplement et à plus grande ampleur. A cette époque, le maitre mot est « curiosité », le hacking est perçu comme une forme de jeu qui peut s'avérer dangereux. L'exemple régulièrement amené est le film « War Games » de 1983 qui présente un jeune adolescent entrant par erreur dans le système informatique de l'armée et manquant de causer une guerre nucléaire. (Holt, T. J., 2020)

C'est à partir des années '80 que la vision des hackers dans la société se ternit. En 1981, I.B.M. démocratise l'utilisation des ordinateurs domestiques. Les risques précédemment perçus deviennent plus

[3] Traduction personnelle des termes utilisés par Peter N. Grabosky, 1998. *Crime in the digital age: Controlling telecommunications and cyberspace illegalities*

importants et effraient parfois. Le hacking devient alors une problématique à laquelle la société essaie de faire face par la création des premières lois ainsi que par l'arrestation de figures-clefs de cette sous-culture comme Kevin Mitnick, alias « le Condor » ou Bill Landreth. Une rupture se crée alors entre les hackers que Loyd Blankenship, alias « le Mentor », décrit dans le *Hacker Manifesto* en 1986 comme des jeunes désireux d'apprendre à contrôler la technologie peu importe les moyens, légaux ou non, afin de perfectionner son utilité pour la société et la société qui voit les activités de hacking comme de plus en plus dangereuses. La création de lois anti-hacking entraînera une perspective plus économique à ces activités. Sur une extrémité, c'est l'apparition des premiers hackers mus par des motivations purement économiques, sur l'autre, c'est la survenance des entreprises de cybersécurité sur le marché de l'emploi. (Taylor, P. A., 1999)

L'Internet se démocratise de plus en plus et, avec lui, les risques perçus par la société grandissent. Selon Klaus Schwab (2017), nous serions entrés dans une quatrième révolution industrielle caractérisée par l'évolution toujours plus rapide des technologies qui font de plus en plus la connexion entre le physique, le biologique et le numérique. C'est notamment la création de *l'Internet of Things* ou de l'Intelligence Artificielle et des risques criminels qu'ils présentent. C'est aussi dans cette ère où l'Internet, omniprésent, devenant un domaine d'importance pour les acteurs politiques qui l'utilisent pour diffuser leurs informations, se faire connaître ou pour obtenir des fonds, qu'un nouveau type de hacking émerge, le hacking idéologique dans lequel certains auteurs mettent le cyber-terrorisme, le hacktivisme ou le hacking d'Etat. (Yar, M. & Steinmetz, K. F., 2019).

Ainsi, en regardant à l'histoire du hacking, on comprend que la définition que Peter N. Grabosky (1998) apporte manque peut-être de recul, puisque l'intention criminelle n'apparait réellement que dans les années '80 pour une partie de hackers et que la connotation négative qui le caractérise aujourd'hui n'est pas représentative de son histoire ou de ses origines poussées par des valeurs d'apprentissage et d'enrichissement de la société. Cela ramène donc la définition du hacking dans cette étude à celle que proposent Oliver DeJarvis, & Adriane, B. Randolph (2022) : « *un utilisateur qui souhaite gagner accès à une cible identifiée (e.g., une entreprise, un réseau, …) dans l'espoir d' 1) apprendre plus sur cette cible 2) de l'exploiter pour une attaque 3) ou pour le bien de la société*. »[4] Evidemment, cette définition reste très large et, même si elle rend compte des différences qui peuvent exister entre différents acteurs de la scène du hacking, il semble important de l'inclure dans une classification permettant de distinguer les différents types de hackers et de préciser l'unité d'observation de cette étude. Cela est l'objectif de la section suivante.

2.1.2. Typologies des hackers

Il existe plusieurs façons de classer les différents types de hackers : la première consiste à ranger les hackers dans des catégories d'activités. Ainsi, Chng & al. (2022) construisent 13 activités auxquelles les hackers peuvent participer. Celles-ci sont fonction de la compétence nécessaire mais aussi du type de motivation qui peut pousser à se lancer dans ce comportement, ainsi que de la façon dont l'attaque peut être faite par chaque type de hacker. Bien que cette typologie soit extrêmement intéressante, il semble compliqué de pouvoir y ranger distinctement chaque individu sans qu'il n'existe de possible chevauchement d'activités. De plus, pour l'étude ici réalisée, il semble impertinent d'utiliser ce type de classement où les hackers légaux se retrouvent seulement dans la catégorie des *Old Guards* (« Hackers qui ne hackent pas pour des raisons malicieuses mais qui n'ont pour autant aucun respect pour la vie privée ») et où ils sont confondus avec des acteurs moins légaux qui exerceraient les mêmes activités. Il est alors perceptible que cette typologie ressort plutôt d'une analyse des hackers illégaux que du hacking tel que défini par cette présente étude.

[4] Traduction personnelle des termes utilisés par DeJarvis, O. & Adriane, B. Randolph, 2022. Hacker definitions in Information Systems Research. P.7. : « a user who wishes to gain access to an identified target (e.g., a company, group, or network) in hopes of 1) learning more about the target, 2) exploiting the target for attack or 3) to benefit society. »

La deuxième provient de Turgeman-Goldschmidt (2008) qui a démontré que la perception que s'auto-appliquent les hackers est aussi sujette à opposition. Ainsi, il remarque que les hackers se distinguent en tant que « bons hackers », qui ont des compétences poussées en technologie, qui ont généralement appris par eux-mêmes, par curiosité, qui sont des acteurs de la lutte pour que la technologie façonne le bien-être de la société et en tant que « mauvais hackers » parfois aussi appelés les *crackers* pour éviter la confusion. Ces crackers sont généralement d'abord mus par des volontés de gains économiques, se disent être talentueux de nature et admettent généralement que le hacking fait partie d'une déviance générale dans leur vie. Cette typologie basée sur une perception de la bonté d'un hacker semble également intéressante, néanmoins, puisqu'elle concerne une auto-perception, elle semble difficilement opérationnalisable dans cette étude. De plus, son étude s'intéressait aux hackers dans un sens plus large, à savoir des individus exerçant tant des activités de piratage digital, de phreaking ou de hacking. Dans le cadre de la présente recherche, le hacker se rapporte à l'individu exerçant le hacking tel que défini plus haut. Finalement, il semble improbable qu'une différenciation plus objective entre hackers et crackers soit aussi manichéenne.

Puisque cette étude s'intéresse principalement à l'aspect humain plutôt qu'à leur activité, il a été décidé d'utiliser une troisième typologie classique qui distingue les hackers dans 3 catégories, à savoir, les *black*, les *grey* et les *white hat* hackers. Les *black hat* hackers correspondraient aux *crackers* définis plus haut : « *des individus qui agissent tant illégalement que malicieusement sur des victimes (une entreprise, une organisation ou un individu), soit seul, soit en réseaux* » (Jaquet-Chiffelle, DO., & Loi, M., 2020). Les *white hat hackers* sont, à l'opposé, « *des individus qui agissent légalement et essaient d'attirer la confiance des entreprises ou organisations qui s'achètent leur service* » (*idem*). Les *grey hat* hackers seraient finalement inscrits quelque part entre les deux, ni totalement blancs, ni totalement noirs : « ils n'essaient pas d'attirer la confiance des entreprises ou organisations ; ils peuvent agir illégalement si cela est nécessaire dans l'atteinte de leur objectif mais n'agissent pas malicieusement et essaient de minimiser les dégâts » (*idem*). Puisque cette étude se veut comme objectif d'étudier la désistance, il semble logique d'exclure la catégorie des *black hat* hackers qui se veulent toujours ancrés dans la cybercriminalité. La catégorie des *white hat* hackers convient d'être conservée au vu de leur définition. Quant aux *grey hat* hackers, puisqu'ils naviguent entre les frontières de la légalité, il revient d'en garder une partie et d'en exclure une autre. Au vu de ces difficultés, la prochaine section tend à vouloir préciser finalement sur quelle population cette étude se basera.

2.1.3. Terminologie utilisée

Au travers de multiples lectures, il semble fréquent d'utiliser le terme *Ethical Hacking* pour désigner un hacker qui s'engage dans l'analyse de vulnérabilités et de protection de celles-ci (Chang, L. YC. & Whitehead, J., 2022 ; Nicholson, S., 2019 ; Zand, E. & al., 2021 ; Del-Real, C. & José Rodriguez Mesa, M., 2023). Pourtant, en 2001 déjà, Richard Barber indiquait : « *personnellement, je trouve ces termes problématiques car ils rendent une mauvaise impression. L'équivalent serait d'appeler les policiers des "cambrioleurs éthiques" ou "voleurs au chapeau blanc"*. »[5] Sa vision rentre bien dans une définition du hacking au sens de Peter N. Grabosky (1998) présentée plus haut et n'est donc pas partagée dans cet article, néanmoins, cette appellation semble rester problématique à deux égards au moins :

D'abord, le terme « éthique » paraît renvoyer au fait que chaque « hacker éthique » serait, inévitablement, porté par son éthique. Or, comme l'ont démontré Jaquet-Chiffelle & Loi (2020) dans leur chapitre *ethical and unethical hacking*, de nombreuses éthiques peuvent être soumises à une forme de compétition, l'une ou l'autre pouvant alors prendre le dessus et faire dévier le « hacker éthique » de son éthique de base pour rejoindre plutôt celle de l'entreprise qui l'engage, par exemple. Ainsi, dans un premier temps, il semble important de relever que l'éthique n'est pas chose immuable, ou binaire, que

[5] Traduction personnelle des termes utilisés par Barber, Richard. (2001). Hackers Profiled — Who Are They and What Are Their Motivations? : « Personally I take issue with these terms as I think they give the wrong impression. The equivalent is to call police officers 'ethical burglars' or 'white hat thieves' »

l'on aurait ou non mais qu'il est bien un concept plus vague et plus général qu'il ne pourrait l'être cru. De la même façon, Levy (1984) a été le premier à montrer que les hackers (aussi bien les *white hat*, que les *grey hat* ou les *black hat*) étaient animés d'une éthique qui rassemblerait entre autres : le droit à l'accès gratuit à l'information, une croyance de l'avancée technologique comme synonyme d'amélioration des conditions sociétales, une relative méfiance envers les autorités, un attrait pour le non-conventionnel et une croyance en une forme d'organisation sociale plus méritocratique. En ce sens, il devient alors apparent que tout hacker est, en réalité, porté par une éthique.

Ensuite, les hackers éthiques sont souvent considérés comme une sous-catégorie des *white hat* hackers. Or, dans une étude portant sur la régulation du hacking éthique en Espagne, Cristina Del-Real & María José Rodriguez Mesa (2023) y associent trois activités différentes : les postes d'entreprises, les *bug bounty hunters* et la divulgation coordonnée de vulnérabilité. Les postes d'entreprise permettent à un hacker légal d'aller tester le système informatique de l'entreprise afin de détecter de potentielles failles, de le consolider, ou de le protéger. Il est alors spécifiquement lié à une entreprise. Ce cadre correspond donc plutôt aux *white hat* hackers. Les *bug bounty hunters* prennent plusieurs formes, soit ils sont mis en place par les entreprises-mêmes (e.g. Facebook, Google, …), soit autour d'une plateforme intermédiaire entre entreprises et *bug bounty hunters* (e.g. HackerOne, Bugcrowd, …), soit au travers d'intermédiaires privés qui achètent les vulnérabilités provenant de hackers illégaux (e.g. Zerodium par exemple). Dans ce cadre de contrat plutôt ponctuel, il semble possible que des *white hat* hackers ainsi que certains *grey hat* hackers soient concernés. Finalement, la divulgation de vulnérabilités coordonnées où les vulnérabilités sont trouvées à l'initiative du hacker légal et qui sont rapportées à l'entreprise concernée ou un intermédiaire. Généralement, les acteurs conviennent d'un plan de réparation de la faille et, au terme d'une durée déterminée, la vulnérabilité est diffusée au public. Dans ce cas, puisque la recherche préalable de faille dans un système informatique n'est pas commandée, elle est une intrusion non autorisée dans un système informatique animée d'une bonne volonté de renforcement d'un système lacunaire et, ce faisant, concernerait donc plutôt un cadre lié aux *grey hat* hackers. Il est donc visible que le hacking éthique, en pratique, vise une portée plus large que celle déterminée par son cadre initial et rejoint plutôt la définition qu'en fait Alana Maurushat (2019) : « *l'utilisation non-violente d'une technologie à la poursuite d'une cause, politique ou autre, qui est souvent légalement et moralement ambigüe* »[6].

Ainsi, cet article postule que « l'éthique » entendue dans le terme de « hacker éthique » porte à confusion puisqu'elle renvoie à la norme de la société à laquelle il faudrait se soumettre plutôt qu'à ce qui pourrait être appelé un « code de conduite ». De plus, la visée du hacking éthique décrite par Cristina Del-Real & María José Rodriguez Mesa (2023) correspond plutôt à la catégorie de la légalité schématisée par Jaquet-Chiffelle & Loi (2020) :

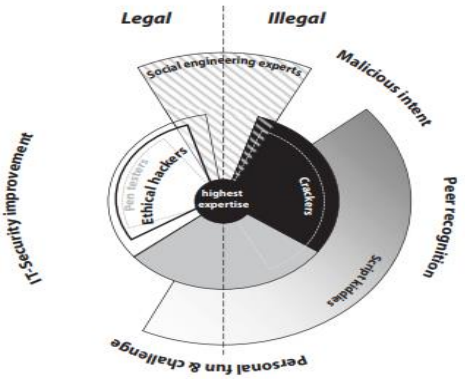

Figure 1 : Schéma de différenciation entre hacking légal et illégal de Jaquet-Chiffelle & Loi (2020)

[6] Traduction personnelle de Maurushat, A. (2019). Ethical Hacking. *CEH v10 Certified Ethical Hacker Study Guide*. p.22 :"*Ethical Hacking* is the non-violent use of a technology in pursuit of a cause, political or otherwise, which is often legally and morally ambiguous."

Au vu de ces confusions, il semble alors plus pertinent, s'il est fait référence à une norme sociétale, de se baser sur le concept de légalité. Ainsi, il devient indispensable de pouvoir séparer ce qui est permis par la loi et ce qui y est interdit. Au vu de cette recherche limitée en temps et en place, néanmoins, il semble impossible d'approcher la réalité juridique de chacun des pays étudiés. Pour se raccrocher à un point qui associerait les différents textes juridiques nationaux, une définition est créée à partir de la Convention sur la Cybercriminalité (2001). Cette Convention trouve son origine dans les travaux du Conseil de l'Europe, une organisation internationale rassemblant (malgré son nom portant à confusion) tant des Etats d'Europe que du reste du monde. Ainsi, 26 Etats de l'Union Européenne (à l'exception de l'Irlande) et 50 Etats du reste du monde ont signé et ratifié cette convention, la rendant ainsi liante et dont la conséquence est qu'elle puisse s'appliquer directement dans ces Etats. L'article 2 de la Convention indique au sujet du hacking que « *chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne,* ***l'accès intentionnel et sans droit à tout ou partie d'un système informatique****. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique*. » Cet article permet, en plus de donner une définition large des comportements concernés, de préciser que chaque Etat dispose d'une marge de manœuvre dans la définition nationale de cette infraction. Ainsi, par opposition, le hacking légal serait admis comme étant un « *accès intentionnel et avec droit à tout ou partie d'un système informatique* ». Cette définition semble entrer en concordance avec les 3 activités précédemment décrites à l'exception de la divulgation coordonnée de vulnérabilité où, dans certains cas, la découverte initiale de la vulnérabilité provient d'une intrusion sur un système informatique. Il existe cependant à cet effet, dans certains pays, une cause de justification retirant le caractère illicite de cette intrusion selon certaines conditions. Cette cause n'est indiquée qu'à titre d'information puisqu'elle dépasse le cadre de cet article[7].

Pour étudier correctement la question de recherche présentée dans cette étude, il semble convenir de n'étudier ainsi que les hackers légaux qui ont fait de la légalité leur métier. Ceux-ci pouvant alors correspondre tant à des hackers associés à une entreprise ou à des hackers qui opèrent des *bug bounties* ou des divulgations coordonnées de vulnérabilité soit au sein d'agences ou pour leur propre compte ou de métiers intrinsèquement associés (enseignement, recherche, …). L'intérêt est de partir d'un échantillon théoriquement composé de *white hats* hackers pour vérifier notamment l'arrêt d'activités illégales, correspondant au concept de désistance primaire[8].

2.1.4. Motivations des hackers

Les motivations des hackers ont surtout été étudiées auprès de hackers illégaux. Il existe notamment une méta-analyse de Chung & al. (2022) sur les types et motivations des hackers illégaux qui montre que les hackers illégaux peuvent se lancer dans ces activités pour des raisons économiques, par curiosité, pour la notoriété, par vengeance, par loisir, par idéologie ou par pulsions sexuelles pour ce qui est des perpétrateurs d'infractions sexuelles en ligne. Ce que montrent également nombreuses autres études (Holt, T.J. & al., 2020a ; Steinmetz, K. F., 2015 ; Jordan, T. & Taylor, P., 1998 ; Holt & al., 2020b ; Denning, D. E., 2011 ; …). Une autre motivation importante à relever revient souvent dans le domaine du hacking illégal : le *thrill*, une forme d'excitation intense ressentie à la suite de comportements risqués ou après avoir résolu un défi, mis en avant par Jack Katz (1988), puis par d'autres auteurs en ce qui concerne le hacking (Van Beveren, J., 2001 ; Noordegraaf, J. E. & Weulen Kranenbarg, M., 2023 ; Steinmetz, K. F., 2015 ; Turgeman-Goldschmidt, O., 2008 ; Palmieri, M. J., Shortland, N., & McGarry, P., 2021 ; Jordan, T., & Taylor, P. H., 1998 ; …)

[7] Pour plus d'informations, voir Enisa. (2022). *Coordinated vulnerability disclosure policies in the E.U.*. Disponible à l'adresse Coordinated Vulnerability Disclosure Policies in the EU — ENISA (europa.eu)

[8] Parfois appelé « désistement » dans le reste de l'article.

Moins d'études cependant viennent interroger les motivations des hackers légaux : on compte parmi celles-ci surtout des rapports d'organisations tels que celui de Bugcrowd (2021) qui indique que la motivation principale des hackers légaux est de combler les failles de systèmes informatiques et d'aider les entreprises à ne pas subir de dégâts de réputation, ou de HackerOne (2021) qui indique plutôt une volonté d'apprendre, de se faire de l'argent, de se créer une réputation et, seulement en quatrième place, de protéger les systèmes informatiques. Une seule étude scientifique de Noordegraaf, J. E. & Weulen Kranenbarg, M. (2023) semble s'en être préoccupé. Ce qu'elles ont constaté après une série d'entretiens semi-structurés avec 15 individus hollandais engagés dans le hacking légal est, d'une part, qu'ils partageaient certaines caractéristiques liées au *thrill* ou à la curiosité avec le hacking de façon générale qui leur permettaient, dans un premier temps de s'intéresser à ce domaine. Néanmoins, dans leur échantillon, ces motivations se sont vites estompées pour laisser place à d'autres liées au hacking légal. Leur motivation primaire en ce sens était de sécuriser les systèmes informatiques en « (…) *prévenant la fuite de données sensibles, en aidant les utilisateurs, en prévenant la fermeture d'un site web, en protégeant les autres et en informant les propriétaires des systèmes [vulnérables]* »[9]. Les participants affichaient ensuite un besoin de reconnaissance/de notoriété plus important à un jeune âge ou en début de carrière. En troisième lieu, certains *bug bounty hunters* admettaient être motivés par une forme de récompense à leurs efforts. Finalement, quelques hackers légaux donnaient aussi des motivations à arrêter cette activité, à savoir, le manque de temps à réserver à la détection de vulnérabilités ou la perte d'intérêt lié à l'activité.

2.2. La désistance

La désistance est un concept maintenant connu de la criminologie. Son intérêt dans le domaine est souvent associé à l'émergence de la théorie des parcours de vie de Sampson & Laub (1993). Néanmoins, le concept a évolué en 30 ans et la Science ne semble pas former de consensus sur une définition claire de la désistance. Il semble en ce sens important de revenir sur ce qu'elle signifie dans cette étude en abordant les contours théoriques qui ont été sélectionnés ainsi que de traiter du (faible) état de la recherche de la désistance du hacking.

2.2.1. Approche théorique

De façon générale, la désistance est maintenant reconnue comme un processus. A cet effet, les travaux de différents auteurs ont mené à une classification de la désistance en 3 phases : la désistance primaire correspondant à la cessation de l'activité délinquante, la désistance secondaire correspondant au passage de la non-délinquance vers une identité non-délinquante (deux concepts de Maruna, S. & Farrall, S., 2004) et la désistance tertiaire qui met en avant la reconnaissance sociale du changement et le développement d'un sentiment d'appartenance (McNeill, F., 2016). Ces mêmes concepts ont aussi été appelés « désistance du comportement », « désistance identitaire » et « désistance relationnelle » par Nugent, B. & Schinkel, M. (2016).

Au sein des théories de la désistance, l'approche qui semblait la plus adaptée à la question de recherche est la théorie de la transformation cognitive de Peggy, C., Giordano & al. (2002) qui se fonde sur des bases de perspective féministe, en implémentant les concepts d'intersectionnalité et d'agentivité. A leur sens, la désistance peut s'envisager sous 4 types :

Le premier est un **basculement dans l'ouverture au changement** du délinquant auquel Giordano & al. (2002) : une première étape dans le changement identitaire de l'individu qui se sent prêt à changer et à se tourner vers la norme. Les auteurs y associent deux caractéristiques intrapersonnelles : une intention

[9] Traduction personnelle de Noordegraaf, J.E., & Weulen Kranenbarg, M. (2023). Why do young people start and continue with ethical hacking? A qualitative study on individual and social aspects in the lives of ethical hackers. *P. 12 :"Their goals with ethical hacking are) preventing the leakage of sensitive data, helping people, preventing a website from being taken down, protecting others, and informing the system owners."*

de désistance, nécessaire mais non suffisante, liée à un plan valable et réalisable de construction de leur futur : Giordano & al. ont effectivement remarqué que l'envie seule de changer permettait rarement d'entamer un processus de désistance et que les participants qui n'avaient pas un programme clair ou réaliste retournaient plus rapidement vers leur mode de vie délinquant. Ils remarquent, par ailleurs, que la plupart des individus interviewés qui avaient désisté parlaient de leurs actes illégaux au passé en mettant une distance par rapport à leur vie actuelle, comme pour créer une séparation narrative entre leur vie d'avant et leur vie actuelle.

Le second est une **exposition à des *hooks for change***. Ceux-ci sont définis comme des opportunités de changement qui peuvent se présentent à chaque individu. Peggy, C., Giordano & al. (2002) les ont étudiés sous 2 formes plus contextuelles : formels – l'importance de la religion ou de l'institution pénitentiaire – et informelles – la parentalité et les relations amoureuses. Néanmoins, ils indiquent déjà l'intérêt qu'il pourrait y avoir à étudier un métier comme une opportunité de changement. Au sens des auteurs, ce n'est pas tant le *hook for change* qui permet le changement mais plutôt les outils qu'il apporte à l'individu pour se prendre en mains dans un mode de vie moins déviant, ce qu'ils appellent un plan cognitif : ce n'est par exemple pas le passage par un traitement qui permette à un individu de s'en sortir mais plutôt ce qu'il aura appris sur lui-même de cette phase de traitement qui lui donneront les clefs pour mieux s'adapter à son nouveau mode de vie.

Le troisième est le fait de **s'envisager un nouveau « soi de remplacement » plus conforme ou plus conventionnel**. Le changement s'opère ici directement dans l'identité qu'un individu se donne. L'idée est que l'identité structure un individu et oriente ses actions. Ainsi, une personne qui s'attribuera une identité positive ou correspondante à la norme aura tendance à aligner ses comportements avec celle-ci ou à refuser de prendre part à des comportements déviants.

Le quatrième type, finalement, est une **transformation de la perception de l'auteur sur le mode de vie déviant ou sur le comportement déviant**. C'est ici un changement de perception plus global qui s'opère sur le mode de vie précédemment vécu. Ainsi, un individu qui parviendra à associer l'acte déviant à des caractéristiques négatives aura tendance à refuser de retourner vers ce mode de vie.

Evidemment, tous ces types sont reconnus comme s'impactant les uns les autres comme le montre ce schéma de Giordano & al. (2002) :

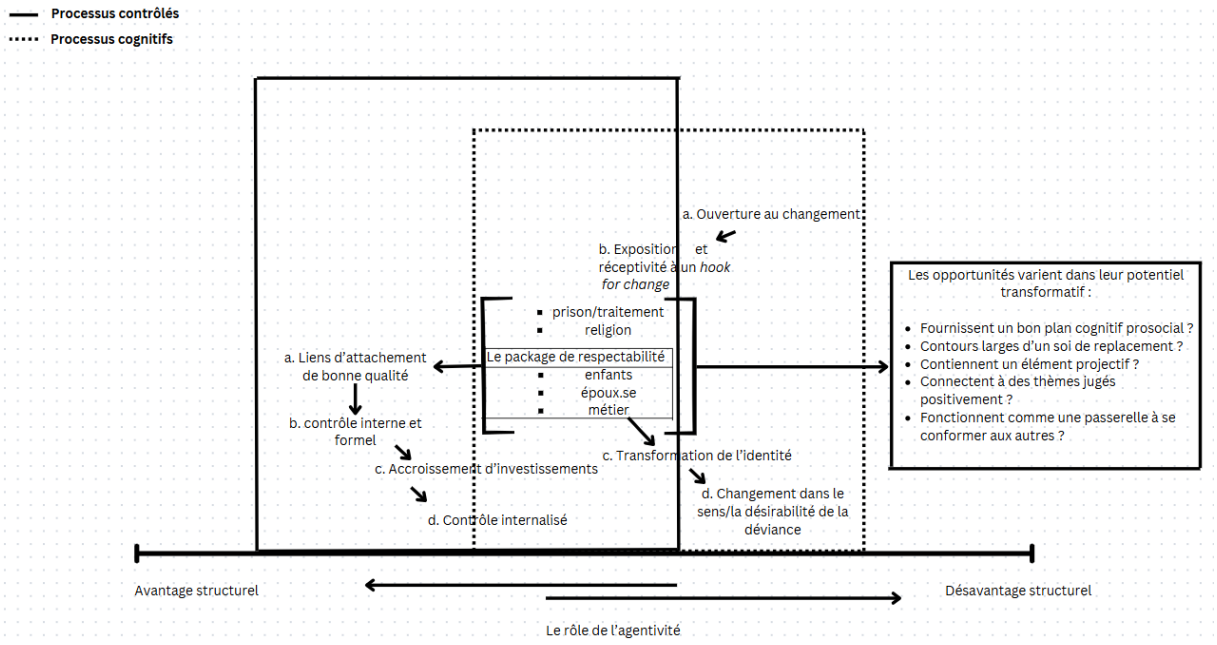

Figure 2 : schéma de la théorie de la transformation cognitive de Giordano & al. [Traduction personnelle] (2002)

Un *hook for change* qui se présenterait à un individu déviant n'aurait, par exemple, que peu d'effet si ce même individu n'était pas ouvert au changement, mais, à l'inverse, un *hook for change* pourrait aussi

amener l'individu à questionner son ouverture au changement ou à envisager un futur plus conforme à la norme, c'est donc ici que l'agentivité joue un rôle important : ce qui semble s'imposer à l'individu fait tout de même l'objet d'une décision personnelle de sa part. Dans le cas d'un métier légal, par exemple, il revient à l'individu d'accepter l'opportunité de ce poste et de s'y tenir. L'idéal étant alors que chacun de ces types de transformation cognitives se suivent et s'établissent à tour de rôle. De plus, ce qui est particulièrement important est que chacun des types de transformation cognitive aura aussi un effet d'orientation du comportement de l'individu. Chaque transformation aurait la possibilité de permettre à l'individu de s'orienter vers un futur plus conforme à la norme ou, à tout le moins, de ne pas s'orienter vers un mode de vie déviant qui serait en opposition à la transformation qu'il effectue.

La théorie de la transformation cognitive semble alors mettre en son centre le concept de désistance secondaire, la désistance identitaire. Néanmoins, elle n'essaie pas pour autant d'en expliquer l'origine causale, notamment au niveau du premier type où les auteurs effectuent plutôt une description de l'ouverture au changement sans essayer d'expliquer pourquoi elle se produit. A cet effet, un complément intéressant semble être apporté par Ray Paternoster & Shawn Bushway (2009) dans le cadre de leur théorie du *feared self*. Celle-ci suppose que les individus sont animés par des représentations de leurs futurs possibles, certaines étant connotées positivement (le soi possible positif), et d'autres, négativement (le soi possible craint). Ces futurs sont alors comparés au présent et peuvent orienter les comportements actuels d'un individu vers l'objectif qu'il se fixe. Selon ces auteurs, néanmoins, « *le mouvement hors d'une identité déviante est plus susceptible, en tout cas, au départ, d'être basé sur une conception de ce que l'individu craint de devenir plutôt qu'une conception de ce qu'il aspire à être* »[10]. Ainsi, un individu qui craint un futur stable dans son statut de déviant pourrait s'ouvrir au changement et accepter la survenance d'un *hook for change* au sens de Peggy, C., Giordano & al. (2002). En outre, ils indiquent que c'est la « cristallisation du mécontentement » -- la prise de conscience de multiples éléments jugés négatifs dans le présent d'un individu et ramenés à son activité déviante ou à son identité – qui permet d'orienter les comportements d'une personne vers de nouvelles opportunités prosociales, ce qui fait vraisemblablement lien au quatrième type de transformation cognitive apporté dans la théorie de Peggy, C., Giordano & al. (2002). En ce sens, il semble alors intéressant de combiner ces 2 approches en ouvrant le questionnement au-delà de l'ouverture au changement de l'individu en s'intéressant à la perception qu'il se fait de la situation de déviance dans laquelle il était afin de mieux comprendre pourquoi, à un moment, il s'est senti ouvert à changer son mode de vie.

Pour aller plus loin, il semble intéressant de constater que la désistance primaire est un concept porté en toile de fond de cette théorie de la transformation cognitive. En réalité, le concept tend à intervenir dès le premier type présenté par Giordano & al. (2002) : le signe d'une ouverture au changement est un début d'arrêt de la criminalité qui permet, par la suite, de suivre les opportunités prosociales offertes. Le changement identitaire de l'individu ne serait donc pas possible si le comportement déviant n'a pas trouvé sa fin. La transformation cognitive agit en ce sens comme une sorte de confirmation de la sortie du mode de vie déviant. De la même façon, les *hooks for change* dans cette théorie ne sont utiles que lorsque l'agentivité de l'individu précède et qu'il a déjà entamé le processus de désistance. En d'autres termes, cette théorie suggère que l'acceptation d'un *hook for change* agit plutôt comme un amplificateur de la désistance que comme un accès à celle-ci. Dans ce cadre, il sera important de questionner la chronologie des évènements de hacking illégaux ainsi que la perception de l'individu sur la diminution de tels évènements afin d'estimer si la désistance suit effectivement cette courbe réductrice de commissions d'infractions à partir de l'accession au *hook for change*.

[10] Traduction personnelle de Paternoster, R., & Bushway, S. D. (2009). Desistance and the "Feared Self": toward an identity theory of criminal desistance. P. 1116 :"(…) movement out of a deviant or 'spoiled identity' is more likely, at least initially, to be based on a sense of what one does not want to become rather than a sense of what one wants to become."

Finalement, la désistance tertiaire, décrite seulement en 2016 par Fergus McNeill, n'apparaît évidemment pas précisément dans cette théorie établie 14 ans plus tôt. Néanmoins, puisque Giordano & al. (2002) traitent déjà de *hooks for change* informels comme la parentalité et les relations amoureuses, il est clair que l'aspect social de la désistance était déjà pris en compte dans l'effet qu'il peut avoir sur l'individu en transformation. Il semble dans ce cas intéressant de prolonger le questionnement en s'intéressant à la façon dont la société voit le changement identitaire de l'individu et si et comment cela peut l'impacter aux différentes étapes de sa transformation cognitive.

En résumé, ces appuis théoriques devraient pouvoir donner une image plus complète de la désistance en se rajoutant à la théorie de la transformation cognitive afin de s'intéresser : 1) aux raisons qui ont permis à l'individu de s'ouvrir à la possibilité d'un changement de vie et d'identité et 2) aux moments où la désistance a démarré et à la façon dont le *hook for change* a joué sur sa continuité, 3) à la vision que l'individu a de son identité, 4) à la vision qu'il entretient du mode de vie déviant en question et finalement 5) en interrogeant les relations sociales de l'individu et l'impact qu'elles ont eu sur son processus de désistance.

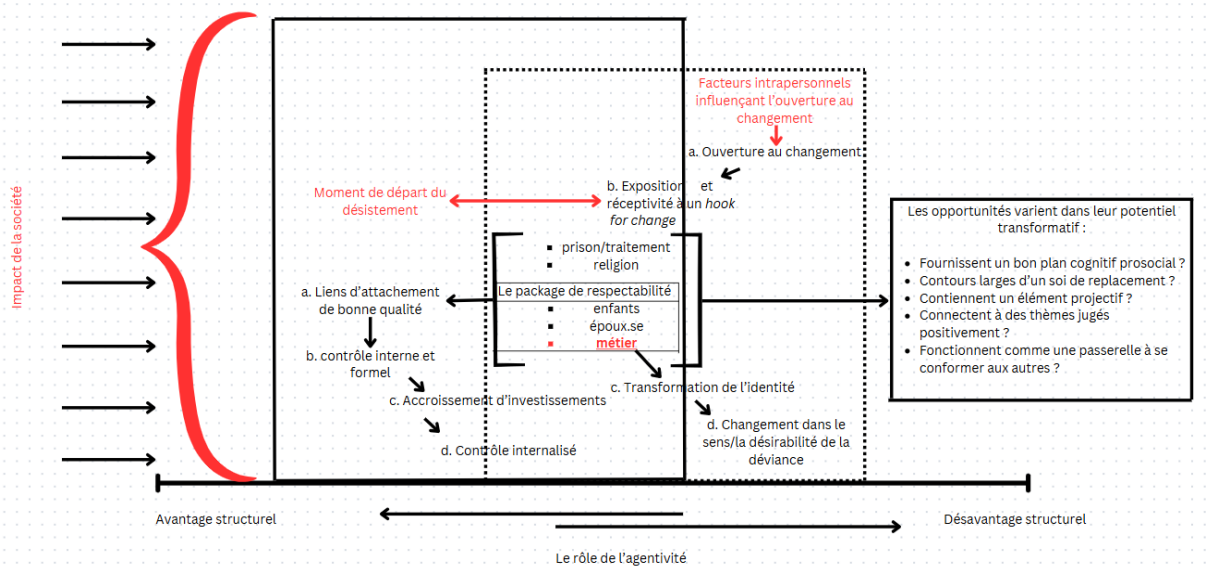

Figure 3 : Version améliorée de la théorie de la transformation cognitive de Giordano & al. (2002)

2.2.2. Revue de littérature

Il est nécessaire de rappeler ici que très peu d'études se sont intéressées à la désistance du hacking. Néanmoins, 3 recherches semblaient intéressantes à mettre en relief dans cette étude :

La première est la revue systématique de littérature de Joeri Loggen, Asier Moneva & Rutger Leukfeldt en 2023 qui met en avant deux éléments d'explication de la désistance liée au hacking : d'une part, la désistance serait le résultat d'une analyse coûts-bénéfices où les coûts deviendraient plus importants que les bénéfices qui y sont liés. A cet effet, les auteurs précisent que cela peut être le cas pour des hackers lorsque le *thrill* vécu s'amoindrit où que le mode de vie déviant commence à trop impacter l'environnement social de l'individu. Ensuite, la désistance serait liée à des effets de maturation au sens notamment de Travis Hirschi & Linda Gottfredson (1983) puisque les jeunes seraient davantage impliqués dans le hacking et cesseraient leurs activités en prenant de l'âge.

La seconde est l'étude qu'ont menée Judith E. Noordegraaf, & Marleen Weulen Kranenbarg (2023), plusieurs observations ont pu être faites sur les aspects sociaux liés à l'engagement d'individus dans le hacking légal. D'abord, tous les participants faisaient part d'un support de leur famille et de leurs pairs prosociaux et assistaient à des rassemblements de hackers, ce qui avait pu les mettre sur la voie du hacking légal. Au niveau du cadre professionnel, la plupart des jeunes obtenait de bons scores à l'école mais y marquaient peu d'intérêt en dehors des cours de technologie. Le premier job ou stage dans un domaine lié à l'informatique semblait être important pour gagner de l'expérience. Dans le cadre des

hackers légaux travaillant sur les activités de divulgation coordonnée de vulnérabilités, un élément indiqué comme favorisant l'implication dans la cause était une réponse positive accordée par les entreprises malgré le flou législatif à ce sujet.

Finalement, un dernier aspect est lié à l'emploi comme *hook for change* et est adressé dans une étude de Torbjorn Skardhamar & Jukka Savolainen (2014) où les auteurs tentent de décrire de façon quantitative l'effet que l'emploi a, ou n'a pas, sur la désistance sur un échantillon de 783 hommes récidivistes ayant eu un emploi entre 2001 et 2006. Une fois les données analysées, ils ont conclu qu'une diminution d'infractions était visible avant la survenance d'un emploi et que l'emploi ne permettait pas de diminuer davantage le nombre d'infractions commises. En ce sens, ils concluaient que l'emploi n'était, dans leur étude, pas à voir comme un facteur causal de la désistance comme tend à le définir le concept de *hook for change* mais plutôt comme une conséquence d'une désistance déjà largement entamée, ce qui reliait plutôt les observations à des effets de maturation.

3. Objectifs et hypothèses de l'étude

Cette étude a ainsi pour objectif d'éclairer le sujet peu étudié de la désistance du hacking et d'analyser le rôle que pourrait avoir le hacking légal comme emploi dans ce processus de désistance à travers la théorie de la transformation cognitive de Giordano & al. (2002). Cette question de recherche se formule alors :

Quelles sont les motivations des hackers illégaux à se tourner vers la légalité et quelle est la pertinence du hacking légal comme vecteur de désistance ?

Au regard de la revue de littérature, plusieurs hypothèses peuvent être faites :

Au niveau des motivations de hackers illégaux à se tourner vers le hacking légal, il est attendu, d'abord, que les participants fassent part d'une morale forte à vouloir protéger les systèmes informatiques et d'une volonté de reconnaissance d'une communauté comme le montrait l'étude de Judith E. Noordegraaf & Marleen Weunen Kranenbarg (2023). Ensuite, que certaines motivations liées au hacking comme la curiosité ou la motivation financière soient aussi comblées par l'acquisition d'un poste dans le hacking légal puisque les activités qui y sont exercées sont similaires, ce qui rejoint Judith E. Noordegraaf & Marleen Weunen Kranenbarg (2023) qui observaient la similitude de certaines motivations liées au hacking illégal dans leur population de hackers légaux. Finalement, que le *thrill* reste une motivation importante à continuer dans le hacking légal plutôt qu'à sortir entièrement du hacking. En ce sens, l'hypothèse va à l'encontre des constats faits par la revue systématique de littérature de Joeri Loggen, Asier Moneva & Rutger Leukfeldt en 2023 qui indiquaient qu'une diminution du *thrill* pouvait mener à la désistance puisqu'ils n'analysaient pas la spécificité de la désistance vers le hacking légal et rejoint plutôt l'étude de Judith E. Noordegraaf & Marleen Weunen Kranenbarg (2023) qui observaient la similitude de certaines motivations liées au hacking illégal dans leur population de hackers légaux.

H1 : Les participants font part d'une **morale forte à vouloir protéger les systèmes informatiques**.
H2 : Le hacking légal et le hacking illégal partagent des **motivations communes**.
H3 : Le ***thrill* reste une motivation importante** à persister dans le hacking du côté légal.

Au niveau de la désistance primaire, il est proposé qu'une diminution d'activités délinquantes soit présente avant l'acquisition d'un poste dans le domaine du hacking légal comme l'indiquaient Torbjorn Skardhamar & Jukka Savolainen (2014). Néanmoins, comme le faisait remarquer Orly Turgeman-Goldschmidt en 2008 : « *Les ex-hackers utilisent toujours leurs compétences lorsqu'ils en ont besoin, bien que pour des raisons tout autres, comme pour obtenir une information que les autres ne possèdent*

pas ou pour gagner un avantage sur un concurrent » (p. 390)[11]. Ainsi, il est probable que certains participants soient toujours par moment engagés dans une conduite déviante. Cela corroborerait néanmoins le premier type décrit par la théorie de Peggy, C., Giordano & al. (2002) où l'agentivité de l'individu et la désistance primaire précèderait la survenance du *hook for change*, ici, l'emploi en tant que hacker légal.

H4 : **Diminution** d'activités délinquantes présente **avant l'acquisition d'un poste**.
H5 : Le hacker légal « repenti » **continuera d'avoir des comportements de hacking illégal**.

Pour ce qui est de la désistance secondaire au travers des trois autres types de transformation cognitive précédemment expliqués, il est suggéré que le hacking légal ne soit pas un emploi comme les autres dans le sens où les activités qui y sont exercées restent techniquement les mêmes que celles exercées dans le hacking illégal mais au travers d'une autorisation. Ainsi, il est postulé que le hacking légal puisse être considéré comme un *hook for change* contrairement aux constats de l'étude de Torbjorn Skardhamar & Jukka Savolainen (2014). Dans ce sens, il pourrait y avoir une diminution d'activités illégales même après s'être tourné vers la légalité si les motivations générales liées au hacking étaient remplies dans un poste légal. L'hypothèse est faite aussi que les postes en entreprises seraient liés à une plus grande réduction d'activités illégales que pour les hackers qui travaillent de façon indépendante sur les *bug bounty* ou sur les activités de divulgation coordonnée de vulnérabilités.

H6 : Le hacking légal est un *hook for change*, il permet ainsi de **diminuer le nombre d'activités illégales après accession à un poste**.
H7 : les hackers légaux en entreprises auraient une diminution d'activités illégales plus importantes que les *bug bounty hunters* et les hackers investis dans les divulgations coordonnées de vulnérabilité.

Au niveau du changement d'identité de l'individu vers un soi plus conforme, il est suivi l'idée de Orly Turgeman-Goldschmidt selon laquelle les hackers (légaux ou illégaux) « (…) *s'assignent le master status 'd'expert informatique' plutôt que celui de déviant* » (2008. p. 393). Ainsi, l'hypothèse est qu'il n'y aura pas de transformation identitaire perçue par l'individu. Pour ce qui est du changement de perception de l'individu sur le mode de vie déviant ou sur le comportement déviant, il est supposé qu'un changement soit opéré au même sens que la « cristallisation du mécontentement » décrite par Ray Paternoster & Shawn Bushway (2009) et que les participants attribuent des éléments de vie négatifs en lien au hacking illégal qui les auraient poussés à se tourner vers la légalité. En ce sens, Mario Silic & Paul Benjamin Lowry (2019) indiquent que la dissuasion portée par la législation anti-hacking pourrait jouer sur les nerfs des auteurs et ainsi les sortir de leur chemin pavé d'illégalité.

H8 : L'accession au hacking légal **ne permet pas une transformation identitaire**.
H9 : L'attribution **d'éléments de vie négatifs liés au hacking illégal** permet de se tourner vers la légalité.
H10 : L'**effet dissuasif de la loi** permet de diminuer le contrôle que les hackers illégaux ont sur leurs nerfs et les mène à se tourner vers la légalité.

Finalement, du point de vue de la désistance tertiaire, il est supposé que la volonté de reconnaissance partagée par les hackers légaux et illégaux amène effectivement les hackers à renouer des liens

[11] Traduction personnelle de Turgeman-Goldschmidt, O. (2008). Meanings that Hackers Assign to their Being a Hacker. P. 390 : "Ex-hackers still use their hacking skills when the need arises, albeit for different purposes, such as obtaining information that others cannot, or gaining an advantage over a competitor"

prosociaux dans un nouvel environnement, lui aussi, prosocial et que cette reconnaissance des pairs soit un élément important dans l'attrait vers la désistance comme l'ont montré Judith E. Noordegraaf & Marleen Weunen Kranenbarg (2023). De plus, selon la même étude, il est attendu que les participants continuent de prendre part à des rassemblements de hackers ainsi que des espaces de discussion. Dans cette recherche, puisque les hackers interrogés auront un passé de comportements déviants, il est alors hypothétisé que certains contacts avec des pairs déviants ou des forums illégaux auront perduré dans le temps.

H11 : L'accession au hacking légal permet de **renouer des liens prosociaux**.
H12 : **Contacts persistants** avec d'anciens pairs délinquants et la communauté du hacking illégal.

Méthodologie

1. Méthode de recrutement des participants

La première étape a été de définir quels types de participants pourraient être amenés à participer à la recherche. Comme la population d'intérêt était complexe à approcher, il a semblé nécessaire de ne pas créer de critères trop précis de participation. Ainsi, comme indiqué précédemment, les personnes recherchées devaient être employées de façon stable dans un emploi de hacking légal (ou, pour rappel, emploi directement associé) pour une entreprise, ou avoir comme activité principale la résolution de *bug bounties* ou de divulgation coordonnée de vulnérabilités tant pour une agence que pour son propre compte. Il n'était pas précisé de durée d'emploi mais il était vérifié que la personne travaille de façon légale depuis au moins 2 ans afin de permettre une analyse de la désistance déjà entamée. Une autre volonté était de ne pas se renfermer sur une zone géographique trop restreinte. Il a donc été décidé de pourvoir à des participants de tous les pays ayant signé la convention cybercriminalité sur laquelle la définition légale de hacking de cette recherche se base, ce qui délimite la recherche à 76 états dans le monde. Une autre restriction concernait la langue parlée : le chercheur ne pouvant parler que français ou anglais, il était impossible de communiquer avec des hackers ne parlant aucune de ces 2 langues. Néanmoins, il semble que cette restriction soit superficielle puisque l'anglais est une langue largement parlée dans le domaine de la technologie. Finalement, pour ce qui concerne le type d'activités illégales dans lesquelles les participants s'étaient essayés, il n'était pas défini de catalogues d'infractions retenues ou non. L'auto-attribution de comportements illégaux étant assez subjective pour les participants, il a semblé plus intéressant de ne fermer aucune porte et de vérifier à posteriori si les activités illégales décrites rentraient effectivement dans la définition de la Convention Cybercriminalité.

Ensuite, il était important de définir les stratégies d'échantillonnage à utiliser pour atteindre les potentiels participants. Deux méthodes non-probabilistes ont été utilisées à cet effet : d'une part, le Centre Cybersécurité Belgique a été contacté pour servir de porte d'entrée vers de potentiels hackers. Un courriel leur a été envoyé en mars 2024 reprenant les informations essentielles à la recherche ainsi qu'un poster[12] regroupant de façon plus visuelle les objectifs de recherche ainsi que les modalités de sélection des participants et les droits leur étant réservés. Le Centre Cybersécurité Belgique a accepté de transmettre l'information à certains de leurs contacts qui rentraient dans les critères. Il leur était demandé de joindre le poster de présentation de la recherche afin de s'assurer que tous les participants potentiels détenaient l'entièreté des informations nécessaires à leur participation à l'étude. Lorsque les personnes intéressées revenaient vers le chercheur, il leur était amené réponses à leurs questions ainsi que plus amples informations sur l'étude et détermination des modalités de rencontre. Un document de consentement libre et éclairé[13] était aussi partagé avant la rencontre afin que le participant soit au courant de ses droits.

[12] Voir annexe 1
[13] Voir annexe 2

D'autre part, une large recherche de participants s'est faite sur internet, sur 2 profils distincts entre février et juillet 2024 : l'intérêt était d'abord de contacter des entreprises de hacking ou dotées d'une équipe de hackers afin qu'ils fassent passer le message à leurs employés et maximiser les chances de contact. Ces entreprises étaient sélectionnées selon une recherche internet pour chaque pays concerné par la recherche. Les entreprises référencées en premier lieu étaient alors choisies par convenance. Plus ou moins d'entreprises étaient contactées en fonction de la taille du pays. Néanmoins, cette méthode a vite montré ses inconvénients car très peu d'entreprises répondaient et, si elles répondaient, indiquaient souvent que leurs employés n'avaient pas participé à quelconque activité illégale. Au vu de ce blocage, il a été décidé de s'adresser directement aux participants potentiels principalement via le réseau social X (anciennement Twitter) mais aussi par Linkedn. Sur ces réseaux, certains mots-clefs liés à la thématique (comme *pentester, penetration tester, hacking, hacker, ethical hacking, legal hacking*) étaient écrits sur la barre de recherche afin de créer une présélection de participants potentiels. Les profils étaient alors analysés rapidement afin d'identifier selon les publications si la personne pouvait répondre aux critères. Si c'était le cas, un message[14] était envoyé qui reprenait des informations sur le chercheur, sur l'étude et sur les modalités de celle-ci et reprenait aussi le poster d'approche. Il était directement indiqué que le chercheur recherchait un participant ayant pris part à des activités illégales dans sa vie (la définition utilisée du hacking illégal était alors jointe au message), ce qui permettait aux personnes non concernées d'être directement identifiées. Cela ressemble néanmoins a posteriori à une erreur car, comme il le sera repris plus loin, il semble que, même si la définition de hacking illégal était donnée, une certaine confusion existe entre hacking illégal et intention bienveillante derrière celui-ci, ce qui a peut-être pu repousser certains participants potentiels rentrant en réalité dans les critères. Afin de contacter un plus grand nombre de personnes, une seconde étape était de rechercher des participants potentiels dans les listes de contacts des personnes trouvées par mots-clefs. Le même processus était alors lancé avec ces personnes et ainsi de suite jusqu'à obtenir une quasi-saturation des profils recommandés par ces réseaux.

2. Méthode de récolte de données

Puisque la question de recherche s'intéresse à une thématique peu recherchée et potentiellement sensible (puisqu'il convient d'avouer avoir participé à des activités illégales qui ne sont peut-être pas connues de l'employeur), il est apparu très rapidement que le meilleur moyen de récolter les données serait de recourir à des entretiens qualitatifs individuels. Les entretiens semi-directifs ont semblé particulièrement intéressants car ils permettaient à la fois de cadrer l'entretien par un guide préétabli autour des hypothèses de recherche et à la fois de rebondir sur certaines thématiques non prévues dans la recherche mais potentiellement intéressantes et émergeant du participant.

Afin de vérifier que le guide d'entretien soit adapté et que les questions inscrites soient pertinentes et bien comprises, 2 personnes ont participé au prétest, l'un étant engagé comme hacker légal dans une entreprise mais n'ayant jamais commis d'infraction de hacking illégal et ne correspondant donc pas tout à fait aux critères de l'étude et le second étant manager technique dans une entreprise et s'occupant d'infrastructure réseaux ainsi que de cyberdéfense et ayant déjà commis quelques faits de piratage, ce qui le fait rentrer dans les critères de sélection des participants potentiels. Néanmoins, il semblait préférable de ne pas utiliser ses données dans cette recherche puisqu'il avait été contacté précisément pour une approche au milieu de la recherche et qu'il avait été établi que ce qu'il dirait ne serait pas partagé. Grâce à ces discussions, le chercheur a d'abord pu se familiariser avec le milieu abordé ainsi qu'avec le guide d'entretien. Ensuite, les questions semblant impertinentes ont pu être transformées ou retirées afin de créer un meilleur outil. Les 2 discussions ont été menées en français, le matériel n'ayant donc pas été prétesté en anglais. Cependant, cela ne semble pas avoir été un problème pour les entretiens en anglais puisque lorsqu'une question était mal comprise, le design semi-directif permettait de la

[14] Voir annexe 3

reformuler. Le guide d'entretien final[15] se décompose en 4 thématiques : les motivations de l'individu, l'influence de son métier dans la pratique du hacking, la perception de son identité et son cercle social. Toutes ces catégories étaient analysées tant avant que le répondant n'ait eu un poste dans le hacking légal qu'après avoir obtenu un tel poste. Les questions posées étaient par exemple : « *comment vous seriez-vous décrit à l'époque ?* » de façon associée à : « *par comparaison, comment vous décririez-vous maintenant ?* » ou bien : « *qu'est-ce qui vous a poussé à vous intéresser au hacking (légal/illégal) ?* » en commun avec : « *Aujourd'hui, ces motivations ont-elles changé ?* ».

Compte tenu de la complexité de la thématique, il était nécessaire d'être flexible sur les méthodes utilisées, ainsi, 2 types d'entretiens ont pu être menés dans cette recherche : les entretiens par visioconférence et les entretiens par mail.

2.1. Entretiens par visioconférence

Kimberly Nehls, Brandy D. Smith, et Holly A. Schneider (2015) ont mis en avant les avantages et désavantages de l'utilisation des entretiens par visioconférence dans les recherches qualitatives. Parmi les principales caractéristiques qu'ils indiquent, il ressort que la discussion en temps réel par l'intermédiaire d'un pc permet d'étendre la zone géographique de recherche ; effectivement, dans le cadre de cette recherche, il est difficilement imaginable de voyager à l'autre bout du monde pour mener un seul entretien, l'utilisation de logiciel de vidéoconférence était alors indispensable. Elle permet parallèlement d'être une alternative moins coûteuse de l'entretien traditionnel ; dans le cas de cette étude qui n'est pas subventionnée, elle apparaît donc comme une excellente option de récolte de données, d'autant qu'elle permet aussi l'accès à l'analyse des signes visuels de l'interlocuteur. Ensuite, elle permet, dans certains cas, de créer une zone de confort pour le participant qui peut choisir l'endroit de la rencontre, souvent, chez lui plutôt que dans une salle d'entretien.

De la même façon, les désavantages qui sont recensés dans cet article semblent ne pas contredire à l'utilisation de l'entretien par visioconférence dans cette étude : les auteurs indiquent par exemple que l'utilisation d'un ordinateur peut mener certaines personnes à se sentir moins en confort, cependant, la qualité des sujets de cette recherche mène à penser que le pc est un de leurs outils quotidiens et qu'ils en ont donc une compréhension certaine. Dans le même sens, l'entretien en temps réel par logiciel n'est possible que si le participant et le chercheur sont équipés d'un ordinateur assez puissant pour faire fonctionner ce type de logiciel ; encore une fois, il semble raisonnable d'imaginer qu'un hacker est effectivement équipé d'un ordinateur assez puissant pour y faire fonctionner un logiciel de visioconférence. Ainsi, l'utilisation d'un logiciel de visioconférence a semblé être le meilleur moyen de mener les entretiens semi-directifs dans le cadre de cette recherche.

Lors de la prise de contact avec les participants potentiels, il leur était proposé que l'entretien se fasse par le logiciel Microsoft Teams tout en indiquant que d'autres alternatives étaient disponibles et discutables. La seule volonté était que le logiciel utilisé soit doté d'un mécanisme d'enregistrement afin de permettre la retranscription par le chercheur. Il était évidemment indiqué au participant potentiel que son anonymat était garanti et que la vidéo ne serait pas utilisée.

2.2. Entretiens par mail

Pour certains participants potentiels, il est vite ressorti que l'idée de communiquer en temps réel par visioconférence était un problème pour leur anonymat ; le chercheur ayant accès tant à leur voix qu'à leur image. Pour d'autres, il semblait compliqué de se libérer pour une interview par manque de temps et à cause de plannings déjà fortement chargés. Ainsi, la méthode d'entretien par mail, aussi appelée *e-interview*, est apparue comme une solution pour ne pas perdre certains participants pourtant intéressés. Celle-ci est perçue comme une forme d'alternative à l'entretien par visioconférence par Roberta Bampton, Christopher Cowton et Yvonne Downs dans un article de 2013 qui leur décrivent néanmoins

[15] Voir annexe 4

une différence majeure : le déplacement ne se fait plus seulement à un niveau spatial, le chercheur et le participant étant à 2 endroits différents durant l'entretien, mais aussi sur un niveau temporel puisque le participant peut répondre lorsqu'il le souhaite au mail sans que le chercheur n'ait la nécessité d'être présent. Cela implique, selon ces auteurs, certaines adaptations : au niveau du participant, puisque l'*e-interview* est asynchronique, le participant peut prendre plus de temps pour réfléchir à ses réponses. L'avantage est une réponse plus complexe ou mieux formulée que s'il avait répondu de façon spontanée mais cela peut parfois retirer le caractère émotionnel d'une réponse, voire permettre au participant de modifier sa réponse afin de complaire au chercheur ou d'embellir la réalité, par exemple. Cependant, le sujet de cette étude n'étant pas spécialement sensible ou empreint d'émotion et demandant même au participant de réfléchir dans son passé, il a semblé que cette méthode soit utile à recueillir des réflexions plus réfléchies de la part des participants. Pour ce qui est de la possibilité de modifier ou d'embellir ses réponses, c'est un risque qui existe similairement avec des entretiens plus 'classiques' et n'a donc pas semblé compromettre l'utilisation de cette méthode.

Au niveau du chercheur, il est recommandé par Roberta Bampton, Christopher Cowton et Yvonne Downs (2013) de traiter l'échange par mails comme une conversation : en limitant le nombre de questions pour laisser la possibilité au participant d'y répondre et d'ainsi mener l'entretien sur plusieurs échanges de mails. Pour les problèmes cités plus hauts quant au planning chargé de certains participants, il est cependant apparu plus judicieux d'envoyer l'entièreté des questions du guide en une seule fois, à un moment déterminé avec le répondant, tout en indiquant la possibilité de revenir sur un second mail pour quelques clarifications : le but étant de permettre aux participants d'avoir directement une idée du temps qu'il leur faudrait pour répondre aux questions sans créer la pression d'un prochain mail ou de risquer qu'ils se lassent au bout de quelques réponses.

Finalement, au niveau de la récolte de données, même si les réponses sont apparues plus concises que celles des entretiens par visioconférence, elles n'ont pas semblé moins pertinentes. De la même façon, il est souvent reproché à l'*e-interview* de ne pas permettre l'analyse de signes visuels. Encore une fois, cela n'est pas apparu comme un problème majeur dans cette recherche qui ne porte pas sur une thématique émotionnelle. Et s'il existait néanmoins quelconque perte d'information à ces niveaux, la méthode permet néanmoins de la balancer en offrant 2 avantages significatifs : la réduction du temps pour le chercheur à mener l'entretien ou à le retranscrire, les réponses étant déjà écrites ainsi que la possibilité de recruter plus de participants. Effectivement, dans le cas où certains hackers n'auraient tout simplement pas participé à cette recherche sans l'utilisation de cette méthode, il est certain que recueillir leurs réponses par mail restait dans tous les cas un meilleur choix que de ne pas les recueillir du tout.

3. Méthode d'analyse des données

Afin d'analyser les données récoltées, il a été fait utilisation de l'analyse thématique, définie par Virginia Braun et Victoria Clarke (2006) comme : « … *une méthode d'identification et d'analyse des schémas de sens (thèmes) au sein d'un ensemble de données* »[16]. Cette méthode en 6 étapes permet une interprétation continue des données au travers de plusieurs relectures et différents niveaux d'analyse : d'abord, en se familiarisant avec les données, notamment par la retranscription des entretiens. Puis en attribuant aux extraits pertinents des codes que Richard E. Boyatzis décrivait en 1998 comme : « *le segment le plus basique, ou élément, d'une donnée brute ou d'une information qui peut être considérée de façon pertinente au regard du phénomène étudié* »[17]. A cette étape, l'analyse reste principalement descriptive, les codes ne font que résumer l'idée principale d'un extrait. Par la suite, les codes se transforment et se rassemblent selon leur point commun en thèmes, ce qui marque le départ d'une analyse plus interprétative. Ces thèmes sont alors réévalués et optimisés avant d'être nommés. La

[16] Traduction personnelle de Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. (p. 6) : « Thematic analysis is a method for identifying, analysing, and reporting patterns (themes) within data »

[17] Traduction personnelle de Boyatzis, R. E.. (1998) *Transforming qualitative information : Thematic analysis and code development.* (p. 63) : « the most basic segment, or element, of the raw data or information that can be assessed in a meaningful way regarding the phenomenon ».

dernière étape consiste à les ranger par ordre de priorité dans l'écriture de l'article afin de répondre le mieux à la question de recherche.

L'analyse thématique n'a pas été soumise à plusieurs chercheurs, ainsi, il est possible qu'un biais de subjectivité existe dans les thèmes relevés et que ceux-ci soient impactés par la personnalité ou les compréhensions du chercheur. Malgré ces potentielles influences personnelles, le travail fourni tente de se rapprocher d'une analyse objective en tentant d'interpréter les différents extraits de la manière la plus fidèle possible.

Résultats

1. Description des participants

La prise de contact initiale a été faite avec 34 entreprises et 102 individus trouvés sur les réseaux sociaux dont 3 personnes ont accepté de participer à cette recherche : 2 par *e-interview* et 1 par entretien par visioconférence. Le Centre Cybersécurité Belgique, contacté comme intermédiaire, a rajouté 2 participants à cet échantillon, tous deux sous la forme d'un entretien par visioconférence. Les 2 entretiens par mails se sont déroulés en un seul échange avec 1 des participants. Pour le second, un second mail a été envoyé pour reformuler une question mal comprise. Quant aux 3 entretiens par visioconférence, ils ont duré entre 1h18 et 2h18. Un de ces entretiens s'est fait en 2 fois pour mieux convenir aux horaires du participant.

L'échantillon total est donc de 5 hommes d'une moyenne de 36 ans et qui occupent des postes de *bug bounty hunter*, de professeur (2), de directeur d'agence de hacking et de *red team operator* en entreprise. Ils sont d'origine française, belge (2), américaine (U.S.) et hongroise. Les participants ont indiqué avoir, entre autres, pénétré dans des systèmes informatiques sans autorisation, notamment des systèmes de votes électroniques, des entreprises, ou des festivals, vendu des numéros de cartes bancaires ou piraté des jeux vidéo. Deux des hackers ont été arrêtés à la suite de certains faits. Au moment de l'entretien, l'ensemble des participants, sauf 1 qui admet toujours avoir des comportements controversés, semble avoir cessé tout comportement illégal.

2. Présentation des résultats de l'analyse thématique

Afin de faciliter la compréhension et la mise en lien avec les hypothèses de départ, les thèmes principaux[18] sont repris et répartis selon le schéma amélioré de la transformation cognitive de Giordano & al. (2002) présenté dans la section de l'approche théorique de la désistance. Pour des raisons évidentes d'anonymat, les noms présentés ont été inventés de toute pièce.

1. Motivations

Loisir

Pour 4 des 5 hackers interrogés, le loisir ressort comme une motivation importante à s'intéresser au hacking, ce qui ressort du témoignage de Philippe :

« *Je voulais m'amuser à pirater des sites comme n'importe quel adolescent qui s'intéresse au sujet* ».

Pour 3 d'entre eux, cette motivation reste même importante encore aujourd'hui, comme le laisse entendre cette anecdote de Thomas :

« Ca fait partie de ton identité, je pense. Pour moi, c'est le côté 'jeu'. Hier, je suis allé dans une friterie où ils ont installé une nouvelle borne de commandes et pendant que j'attendais mes frites, j'étais.. j'ai regardé si je pouvais hacker la borne. Ca a fonctionné mais j'en ai rien fait, j'ai juste fermé l'appli et je me suis assuré que le prochain client puisse commander dessus mais oui, c'est pas quelque chose que tu laisses au

[18] Voir annexe 5 pour le tableau complet de l'analyse thématique

boulot, c'est une mentalité. Quand tu vois des câbles, quand tu vois quelque chose qui peut être hacké, tu le fais juste pour le sport »

Thrill

De la même façon, le thrill est une motivation rapportée par 4 des 5 hackers rencontrés et Stephan va même jusqu'à comparer ce sentiment à la prise de drogues :

« *J'ai jamais pris de drogue, j'ai jamais touché à ça mais j'imagine que c'est un peu la même sensation de tu le fais et puis tu la recherches encore et encore parce que ça arrive pas si souvent de réussir un hack* ».

Encore une fois, pour 3 de ces hackers, ce sentiment perdure à travers les années et reste 'magique' comme l'explique Andrew :

« Arriver à prendre les commandes d'administrateur continue de me fasciner, encore aujourd'hui, peu importe le nombre de fois que je l'ai déjà fait. C'est dingue, c'est 'magique'. Je ressens le frisson quand je fais des choses 'impossibles' »

Curiosité

Pour ce qui est de la curiosité, 3 participants affirment qu'elle était présente dès le début. C'est le cas notamment de Andrew :

« La curiosité. J'étais un enfant intelligent dans une ville de merde où il n'y avait rien à faire » […] « J'ai toujours été un enfant curieux, j'ai toujours voulu savoir comment les choses fonctionnaient »

Pour 2 d'entre eux, cependant, elle tend à s'être calmée et à ne plus être une forme de recherche insatiable, ce que Gabriel met en lien avec l'exercice de son métier :

« Je crois que j'atteins une certaine forme de satiété intellectuelle en termes de résolution de puzzles et de résolutions de petits challenges, entre guillemets, dans le cadre de mon travail et donc je n'ai pas besoin d'explorer ça en dehors »

Pour Stephan, néanmoins, la curiosité n'est arrivée que plus tard, une motivation qu'il lie à son âge :

« Je pense que la curiosité est venue plus tard, en grandissant, quand j'ai commencé à me demander 'pourquoi est-ce que ça fonctionne de cette manière ?' et 'comment ?', alors, c'est vraiment devenu une forme de problème à résoudre plutôt qu'un amassage d'informations pour le pouvoir. »

Liberté

La liberté est abordée par 2 des participants dont Thomas qui compare son activité à une enfance renouvelée :

« J'ai toujours plein d'imagination, de liberté, je peux faire tout ce que je veux et maintenant que j'ai l'argent de le faire, je revis juste plus pleinement mon enfance »

Argent

La question de l'argent a été abordée par 3 des participants qui ont jugé qu'elle n'était pas importante directement dans leurs démarches mais plutôt en filigrane dans leur esprit comme un facilitateur potentiel, Stephan l'explique en disant :

« Donc ouais, y avait toujours cette sorte de, pas vraiment une envie de faire de l'argent, mais de savoir que c'était important pour payer le loyer et d'autres trucs. »

Notoriété

La notoriété était une motivation primordiale pour chacun des participants de l'étude quand ils se sont lancés dans le hacking, comme une forme de validation externe et en reste même une pour Andrew :

« Je pouvais m'en vanter auprès de mes potes et montrer que j'étais intelligent » […] « c'était très important pour moi, et bizarrement, ça l'est toujours. »

Pour les 4 autres participants, la notoriété n'a plus la même importance et est passée à un niveau plus secondaire; ce qui servait plutôt à combler un ego à l'époque semble avoir diminué avec le temps et l'expérience, voici comment Gabriel le ressent :

« Y a aussi le côté réputationnel hein : pendant tes premières années, tu veux t'établir un nom, tu veux que tes postes.. 'fin que tes blogs soient partagés, que tu sois écouté par la communauté, par tes X followers sur Twitter, donc tu bosses, tu bosses, tu bosses pour pouvoir publier un max de trucs. A partir d'un moment, t'as … 'fin, j'ai toujours cette envie de reconnaissance mais j'ai l'impression d'avoir atteint un niveau qui me convient dans le sens où j'ai présenté à des conférences, je donne cours, j'ai publié pas mal de choses et donc j'ai plus ce besoin maladif de 'lisez-moi, lisez-moi, regardez…' »

Pouvoir

3 participants disent aussi rechercher une forme de pouvoir dans le hacking, une façon d'être entendu et respecté comme l'indique cet extrait de Thomas :

« C'est une forme de psychologie : en devenant hacker, tu te fais entendre. N'importe qui va t'écouter si tu dis 'j'ai accès à vos données d'utilisateurs', tout le monde écoutera. Et s'ils n'écoutent pas, ça m'est déjà arrivé dans un festival où j'avais trouvé la line-up des groupes, je les ai contactés, ils ne voulaient pas me croire, du coup je leur ai dit le nom des 5 premiers groupes et là, ils étaient en mode 'oh, il faut qu'on parle' et j'ai répondu 'oui, faut qu'on parle' »

Pour 2 d'entre eux, ce pouvoir est aussi associé à une forme de refuge face à l'injustice qu'ils subissaient dans le monde 'normal', c'est le cas notamment de Stephan :

« Donc, pour moi, c'était vraiment… j'étais un enfant un peu potelé qui était sur le pc et, à ce moment, les pcs n'étaient pas cool donc les gens se moquaient de toi et c'était… mais bon, je rentrais à la maison et j'avais ce pouvoir sur le pc, c'était tout mon monde. C'était vraiment une échappatoire. »

Protection des autres

3 des 5 participants estiment qu'une motivation nouvelle par rapport à leurs débuts dans le hacking est une volonté de protéger les systèmes ou d'être utile aux utilisateurs, ce changement de prisme est décrit par Gabriel :

« Y a une motivation qui a changé aussi, c'est que je construis et conçois plus que je ne casse des systèmes et donc c'est une motivation de… oui, construire quelque chose de A à Z et de le voir fonctionner, de le voir être utilisé par des centaines ou des milliers de gens, donc ça, c'est assez cool »

Pour Andrew, cette motivation était déjà présente depuis toujours :

« Ca a l'air bateau, mais je sais pas, faire quelque chose de bénéfique a toujours été important pour moi. »

Finalement, pour Thomas, la protection des systèmes semble parfois compromettre son propre plaisir à hacker :

« Parfois, c'est même pas fun parce que c'est un peu 'bon, bah je viens de perdre l'accès' »

2. <u>Facteurs modifiant l'ouverture au changement</u>

Peur du risque légal

Les lois ont clairement eu un effet dissuasif sur 4 des participants de la recherche dont Gabriel qui indique qu'elles lui ont permis de définir des limites à ses comportements :

« Oui, je pense que ça m'a clairement arrêté là où il fallait. […] L'optique d'un procès au long cours et de me faire saisir mon matériel et puis de terminer par, je sais pas, même 2 ans de sursis, c'est clairement pas… c'est clairement pas comme ça que je vois le futur, ni maintenant, ni à ce moment-là et donc ça a clairement eu une influence. »

3 d'entre eux estiment même que l'évolution des lois rend la pratique plus sensible et les risques plus grands, comme en atteste Thomas :

« J'aime bien avoir un peu plus de protection mais je fais plus attention maintenant qu'un cadre légal existe. […] Maintenant qu'il existe des lois, je dois y adhérer et elles sont un peu plus rigides que je l'aimerais mais quand c'était un flou légal, je pouvais faire ce que je voulais et je savais que c'était pas illégal dans tous les cas, je me disais 'ouais, je peux le faire' et soit m'en sortir sans problème ou mettre la presse au courant puis la presse aurait choisi mon camp parce que j'étais un peu un genre de Robin des Bois, tu vois, en trouvant une vulnérabilité dans une entreprise qui veut te poursuivre pour ça alors que tu n'en as pas abusé, mais c'était illégal »

Pour les 2 participants restants néanmoins, les lois sont encore trop souples dans leur pays, c'est notamment ce qu'indique Philippe :

« Je pense que les lois ici sont un peu trop souples donc non, je n'avais pas vraiment peur de ça »

Peur de perdre sa situation

Thomas ainsi que 2 autres participants décrivent aussi une peur de perdre leur situation tant professionnelle que familiale :

« Maintenant, je ne fais plus ça parce que j'ai trop à perdre : j'ai une famille, j'ai un job… »

3. Ouverture au changement et opportunité du hacking légal

Hasard

Pour 4 des participants, l'idée de travailler dans le domaine légal du hacking semblait impossible, le fait d'y aboutir étant plutôt associé à une forme de coïncidence, ce qui transparaît dans le discours de Philippe :

« Je n'avais aucune idée à l'époque qu'il pouvait y avoir du hacking légal, l'activité était encore peu développée à l'époque, et c'était plus une passion pour moi au départ, donc je ne pensais pas travailler là-dedans un jour »

Appréhension

3 participants décrivent une peur qu'un métier 'de bureau' transforme le plaisir qu'ils ressortent du hacking, ce qui explique les postes plus indépendants qu'ils ont choisis d'occuper, jusqu'à marquer parfois une vraie répulsion à des jobs plus exécutifs comme les testeurs d'intrusions en entreprises, ces extraits du discours de Stephan sont explicites :

*« Dès que c'est devenu un métier, ça a perdu l'essence de ce que c'était. C'est devenu cette sorte de hiérarchie et plus cet environnement fun et pleinement anarchiste. C'était devenu une structure. […] C'était quelques années vraiment bizarres parce que y avait quelque chose d'amusant à hacker mais… en même temps le faire comme carrière était… j'ai vraiment détesté et c'est pour ça que… c'est aussi à ce moment que je me suis dit 'okay, peut-être que je suis pas fait pour travailler en équipe' ou pour travailler pour quelqu'un ou bien des dirigeants stupides qui me disent quoi faire et c'est pour ça que j'ai continué seul. » […] « Rien qu'en le mentionnant [testeur d'intrusion], ça m'a vraiment *imite des signes de crispation* »*

4. Raison d'arrêt du hacking illégal et type d'effet sur le désistement

Maturité

L'entièreté des participants décrit l'influence d'une forme de maturité liée à l'âge dans l'explication de l'arrêt de comportements illégaux. Aucun ne la décrit comme un tournant dans leur mode de vie mais elle semble jouer un rôle plutôt secondaire dans la vie de chacun. Dans ce cadre, il semble que le désistement se fait de façon graduelle, l'exemple le plus flagrant est donné par Gabriel :

*« Y a une certaine forme de jeunesse aussi hein *rire* dans la manière d'aborder tout ça et dans la manière de se lancer sur certaines choses. Je pense qu'il y a une … une forme de maturité de réflexion, 'fin… j'ai pas envie d'être… d'apparaître comme un jeuniste ou quoi que ce soit mais c'est… je suis au contact d'étudiants et y a une certaine forme de genre recklessness quoi, c'est tu bourres dedans et puis advienne que pourra quoi. Donc dans un mode opératoire dans lequel j'étais clairement et qui maintenant ne me qualifie plus trop quoi… »*

Arrestation

Pour les 2 participants qui se sont fait arrêtés, il semble que le moment de rencontre avec la justice a été déclencheur du désistement de façon directe, comme l'atteste Philippe :

« [Ma perception du hacking illégal] a changé pendant mon arrestation, donc bien avant [d'avoir un métier], les policiers qui m'ont arrêté à l'époque étaient sympathiques, ils m'ont expliqué qu'il y avait mieux à faire que de faire du hacking illégal et j'ai donc suivi cette voix »

Métier

Seulement 2 participants parlent de leur métier pour décrire un arrêt des comportements illégaux mais ne semblent pas lui donner une place prioritaire dans ce processus, l'un tendant plus vers l'influence de la maturité et l'autre, Andrew, mettant plutôt son métier en parallèle à d'autres alternatives légales satisfaisant sa curiosité :

> *« Je fais plus vraiment [de trucs illégaux]. Ca fait même un petit temps. Je travaille toujours de mon côté mais dans ce cas, soit je le reporte à l'entreprise et je publie les résultats, soit je le fais pour le fun sur mon propre système. La plupart du temps, hacker mon entreprise arrive à satisfaire ma curiosité »*

Dans les 2 cas, il semblerait que le désistement se soit fait de façon directe plutôt que de façon progressive.

5. Identité personnelle

Continuité de l'identité de 'hacker'

Parmi les 5 participants, 4 décrivent avoir gardé une identité de hacker même après l'arrêt de comportements illégaux, c'est le cas notamment de Stephan pour qui cette identité est restée primordiale tout au long de sa vie :

> *« Je suis toujours un hacker en premier lieu : même en étant ingénieur, je restais un hacker. Mais je suis un hacker en premier et le fait de donner des cours, c'est … c'est mon mode de hacking, je suppose. Je sais pas mais … ouais, je suis définitivement un hacker. Je me suis toujours associé à l'étiquette de hacker plutôt qu'à celle de prof. » […] « Je pense que l'étiquette de hacker est peut-être plus importante maintenant, pas pour une question d'ego, comme j'ai dit au début, j'avais plus d'ego enfant que maintenant. Maintenant, c'est plus que j'ai passé tellement de ma vie à ça : apprendre aux gens les racines et l'histoire [du hacking] »*

Pour 2 d'entre eux, dont Thomas, il existe cependant une différence entre le niveau technique qu'ils avaient à l'époque, où ils se caractérisaient comme des *script kiddies*, et leur niveau actuel de hacker :

> *« Je suppose que j'étais un script kiddie, c'est comme ça que tout le monde commence donc t'as peu de compétence de programmation mais tu veux quand même voir comment les choses fonctionnent et les hacker, je passais à chaque fois quelques étapes importantes, je savais pas toujours ce que je faisais mais je le faisais pour le résultat et ce résultat était vraiment cool » […] « Je suis réellement un hacker et je pense pas le dire pour m'en vanter : être hacker, c'est simplement avoir une forme d'état d'esprit, faire les choses d'une façon que les autres ne feraient pas. Je pense que tout le monde peut être hacker sans être technique, juste en pensant comme un hacker. Donc oui, je suis un hacker de plein de façons »*

Changement d'identité

Pour le dernier participant, Philippe, l'identité de hacker ne convient plus réellement à ce qu'il fait, il se désigne plutôt comme un expert en sécurité informatique :

> *« Je me considérais 'hacker' à l'époque comme tout jeune avec un minimum de connaissances sur le sujet. » […] « Maintenant, je ne me considère plus comme ça, c'est plus un travail d'expertise en sécurité informatique »*

6. Perception du mode de vie délinquant

Objectif du hack

3 participants sont d'accord pour dire que le hacking n'est pas foncièrement légal ou illégal, pour eux, c'est l'objectif du hack qui change, Andrew l'illustre dans cet extrait :

> *« Chaque hack commence de la même façon (à moins qu'il y ait un contrat), la seule différence vient de ce que tu fais de tes découvertes. »*

Importance de l'intentionnalité

Une distinction apportée par 2 participants entre le hacking légal et le hacking illégal est l'importance de l'intentionnalité, pour Andrew, par exemple, le hack par curiosité n'est pas un problème :

« J'ai jamais eu de problème avec les gosses curieux et bien-intentionnés qui font des conneries. J'ai un problème avec ceux qui font des dégâts, en hacking ou ailleurs. »

Impertinence du terme 'hacking illégal'

Gabriel ainsi qu'un autre participant expliquent qu'à leurs yeux, le hacking n'est pas légal ou illégal, mais plutôt que certains hacks sont un crime et d'autres non. La réponse qu'il apporte est empreinte néanmoins d'une difficulté de trouver un terme adapté :

« En fait, techniquement, je ferais pas de différence entre du hacking éthique et non éthique ou illégal et légal dans le sens où, foncièrement, si c'est quelqu'un qui est intéressé par le challenge technique, le puzzle à résoudre ou la vulnérabilité à trouver ou la manière de détourner un objet ou un logiciel de sa fonction première, bah, voilà, pour moi, c'est un hacker qu'il utilise son savoir pour le… en fait, j'ai même pas envie de dire … de parler de bien ou de mal ou de bon ou de mauvais ou de parler d'éthique ou de moral, tu vois, les 2. Je considèrerais de toute façon la personne comme un hacker. » […] « Je serais plus d'utiliser le terme 'cybercriminels' pour les uns et, je sais pas, professionnels de la cybersécurité, peu importe. Mais même du côté de la cybercriminalité, y a .. 'fin, techniquement, c'est des professionnels de la sécurité, c'est juste qu'ils gagnent leur pain différemment quoi. »

Absence de regrets sur les comportements illégaux

Parmi les 5 participants, 2 indiquent ouvertement n'avoir aucun regret sur leurs comportements passés, et cela malgré les conséquences qu'ils auraient pu subir :

« Je changerais rien à ce que j'ai fait et si j'étais allé en prison, ça aurait peut-être un peu changé ma vision des choses… je suis pas sûr que ça l'aurait changée. »

7. Société et impact social

Séparation entre hacking et monde 'normal'

Tous les participants marquaient une importance à avoir un cercle social dans le monde 'normal' afin de pouvoir parfois se séparer de leur passion, comme le présente Stephan :

« Mais c'était, comme j'ai dit, cette séparation : le monde du hacking d'un côté et les gens normaux de l'autre, et je pense que c'était important pour moi, c'était une forme de balance. »

Contact avec des hackers

3 participants décrivent les contacts qu'ils ont avec des hackers de façon générale, pour Gabriel, il semble que le temps et l'expérience ait permis un accroissement des contacts, mais de façon professionnelle :

« Une expansion de mes contacts on va dire dans le milieu de la sécurité, plus d'un côté … expansion plus globale on va dire, c'est plus des gens qui viennent d'un peu partout dans le monde alors qu'avant, c'était peut-être plus centralisé sur la Belgique ou en tout cas l'Europe de l'Ouest. »

Pour les 2 autres participants, dont Stephan, ce même accroissement est apparent mais semble parallèlement lié à une diminution des contacts familiers avec ces hackers, c'est ce dont témoigne Thomas :

« Au plus tu connais des hackers, au plus tu te distancies en quelque sorte » […] « J'ai pas vraiment de cercle social de potes hackers et je pense que c'est pas grave. »

Fréquence de contacts avec des hackers illégaux

En ce qui concerne Philippe, il marque une rupture avec les contacts qu'il a pu avoir dans sa jeunesse :

« Je n'ai gardé aucun contact avec des hackers malveillants, et je suis maintenant seulement observateur et non acteur sur les forums illégaux dû à mon travail principalement »

Pour 2 autres des participants, ils admettent parfois avoir été en contact avec ce type de profil mais de façon ponctuelle sans spécialement rechercher le contact :

« Je visite parfois encore quelques forums pour avoir des infos mais je le fais pas régulièrement. »

Perception externe du hacking

Stephan révèle que, pour lui ainsi que pour un autre participant, le hacking est vu de façon positive par leur entourage, voire crée un engouement, comme le montre cet extrait :

> *« Tu dis à quelqu'un que t'es hacker et ils sont genre 'wow'. C'est tellement cool que la plupart du temps quand les gens me demandent ce que je fais, je dis que je suis ingénieur parce que si je dis que je suis un hacker, maintenant, c'est tellement vu comme quelque chose de cool, même si les gens pensent que c'est illégal, être hacker reste cool et ça peut créer plein de débats donc je dis juste que je suis ingénieur et les gens se disent juste 'oh…' »*

Pour les 2 participants qui ont été arrêtés, aucun stigmate n'en est ressorti, pour Philippe, cela a même été le tournant dans sa sortie de la délinquance :

> *« Au départ, je piratais pour le plaisir puis je me suis fait arrêter et ils m'ont proposé de travailler pour eux ensuite »*

Discussion

L'objectif de cette recherche était de combler le manque de recherches sur le hacking légal ainsi que sur la désistance du hacking. La revue de littérature avait permis de mettre en avant 12 hypothèses à différents stades de l'approche théorique utilisée modifiant la théorie de la transformation cognitive de Giordano & al. (2002). Afin d'avoir un point de vue plus complet sur ces hypothèses, les résultats décrits dans la section précédente seront associés à certains ressentis généraux du chercheur au travers des entretiens menés. Il est cependant nécessaire de préciser ici que cette étude n'a pas pour objectif d'amener des éléments de réponses généralisables mais plutôt d'orienter les futures recherches dans le domaine. Néanmoins, quelques implications légales seront aussi apportées pour essayer de mieux correspondre aux réalités du hacking.

1. Interprétation des résultats à la lumière des hypothèses

1.1 Motivations à se tourner vers la légalité

Le premier intérêt de cette recherche était de s'intéresser aux motivations des hackers à se tourner vers la légalité. Il avait été hypothétisé, à cet effet, que le hacking légal et le hacking illégal partageraient des motivations communes, le *thrill* restant notamment primordial à l'exercice de leur métier, mais que les participants auraient acquis une nouvelle volonté forte à vouloir protéger les systèmes informatiques. Les résultats semblent aller dans ce sens et dans le sens de l'étude de Judith E. Noordegraaf & Marleen Weunen Kranenbarg (2023) puisque les motivations retrouvées chez les hackers rencontrés et similaires aux motivations déjà recensées dans la littérature comme la curiosité, le *thrill* ou le loisir sont ressorties comme étant des motivations importantes tant au moment de débuter dans le hacking qu'au moment d'en faire son métier. Néanmoins, il convient de rappeler que les hackers rencontrés occupaient des postes d'autonomie et qu'ils ne répondaient pas aux volontés de clients, de direction ou d'horaires imposés. Les participants expliquaient d'ailleurs que si c'était le cas, ils craindraient de perdre ce *thrill*, le traitement d'une passion comme un métier semble alors assez complexe.

Pour ce qui est de la notoriété, les autrices indiquaient qu'elle était importante aux premiers moments de hacking mais qu'elle le devenait moins avec l'expérience et, encore une fois, les résultats de la recherche semblent appuyer ces observations. Une autre motivation semble d'ailleurs suivre le même déclin d'importance dans la vie des participants : le pouvoir. En ce sens, il apparaît que la notoriété et le pouvoir (et encore plus lorsque le hacking est utilisé comme refuge) agissent plutôt comme des réponses aux potentielles inégalités et injustices perçues dans la jeunesse des hackers ; injustices personnelles comme le fait d'être harcelé ou peu inclus dans les cercles sociaux à l'école mais aussi injustices sociales comme le manque de crédibilité associé aux paroles des enfants. Grâce à l'âge, et à l'expérience, les

participants n'ont pas paru ressentir ces injustices au moment de l'entretien, ce qui semble marquer qu'ils ont trouvé un équilibre et une place assumée au sein de la société.

Ensuite, la quasi-totalité des participants confirme qu'il existe en eux une place importante allouée à la protection des systèmes ou à aider les autres, semblant encore une fois correspondre aux résultats obtenus par Judith E. Noordegraaf et Marleen Weunen Kranenbarg (2023). Cette volonté est d'ailleurs souvent apparue à la suite d'un déclic dans la vie des personnes rencontrées, souvent par une personne rencontrée et utilisée comme une forme de mentor.

Finalement, il semble important de préciser que le rapport à l'argent semblait, dans cette recherche aussi, n'être placée qu'à un second plan, les participants voyant plutôt leur salaire comme un bonus à faire ce qu'ils aiment plutôt que comme un objectif.

1.2 Pertinence du hacking légal comme vecteur de désistance

Le second intérêt de cette recherche était de savoir si le hacking comme métier pouvait servir comme base à la désistance de hackers illégaux. A cet effet, il semble intéressant de remarquer que les raisons avancées par les participants à s'être ouvert à un changement vers la légalité étaient principalement liées à une peur de ce qu'ils pourraient perdre dans le futur plutôt qu'à une volonté de futur plus positif. Cela rejoint une partie de la théorie du *feared self* de Ray Paternoster & Shawn Bushway (2009) et semble être corroboré par la presque-totalité de participants ayant indiqué que l'accès à un métier de hacking légal était, pour eux, une coïncidence et non une volonté planifiée, d'ailleurs associée à une certaine appréhension de faire du hacking leur métier. La peur de perdre sa famille, de se faire arrêter ou de perdre sa qualité de vie semble, comme le supposaient Mario Silic & Paul Benjamin Lowry (2019), alors plutôt jouer un rôle sur une évaluation des conséquences au sens de Clarke & Cornish (1985) dans leur théorie du choix rationnel et à ouvrir à la possibilité de se tourner vers un autre mode de vie plus conventionnel. En toute logique, puisque l'ouverture au changement imaginée comme la première étape à la désistance selon Giordano & al. (2002) est empreinte d'agentivité du côté de l'individu, il fait sens d'y retrouver ces aspects rationnels.

Si le concept central de la théorie de Giordano & al. (2002), le *hook for change*, fonctionnait avec le hacking légal, les résultats de cette recherche devraient montrer un désistement précédant l'obtention d'un poste légal avec une diminution graduelle des activités illégales commises par les participants après son obtention jusqu'à un désistement total. Cependant, même si les participants affirment effectivement avoir entamé leur désistance avant d'être engagé comme hackers légaux, il semble que leur désistement était déjà abouti au même moment : à l'exception d'un participant ayant eu des comportements à la limite de la légalité après avoir acquis un job dans le domaine, tous ont semblé avoir cessé tout comportement douteux ou toute tentative d'obtention d'informations par moyen illégal, ce qui contredit l'hypothèse de Orly Turgeman-Goldschmidt en 2008 que les hackers repentis pourraient utiliser leurs compétences à des fins personnelles. Néanmoins, il est important de préciser que les évolutions légales amènent un cadre plus précis quant à ce qui est légal ou non par rapport à 2008 et que les divulgations coordonnées de vulnérabilités sont plus fréquentes qu'elles ne l'étaient à ce moment, il est donc plus simple pour les hackers de s'informer ou de découvrir des vulnérabilités sans risquer de sortir de la légalité. En réalité, il apparaît plutôt que le désistement est causé par des aspects plutôt socio-contextuels dans la vie des personnes rencontrées : d'une part, l'importance de la rencontre avec une personne qui a pu les remettre dans une sorte de droit chemin et d'autre part, une forme de maturité prise avec l'âge. Ainsi, les résultats semblent rejoindre ceux qu'observaient Torbjorn Skardhamar & Jukka Savolainen dans leur étude de 2014, qui constataient qu'un métier ne semblait pas pouvoir s'apparenter à un *hook for change* étant donné que leurs participants n'indiquaient pas de déclin de criminalité après l'obtention d'un poste. Le hacking légal ne ferait pas exception à cette observation, ce qui lui donnerait plutôt la place d'une conséquence d'un désistement abouti plutôt que celle d'un levier pour y parvenir.

Au niveau de la troisième étape de désistance du modèle de Giordano & al. (2002), la transformation identitaire vers un nouveau soi plus conventionnel, il apparaît que l'identité de hacker reste chez les

participants une forme de *master status* qu'Everett Hughes décrit en 1945 comme la tendance que les observateurs ont de croire qu'une étiquette ou catégorie démographique est plus importante que tout autre aspect des performances, des comportements et du contexte de vie de la personne observée, c'est-à-dire que tous les participants, à l'exception d'un, donnent une place primordiale à l'identité de hacker dans leur vie, même après avoir cessé tous comportements illégaux. Cela fait d'autant plus sens quand leurs perceptions de leur mode de vie délinquant sont observées en parallèle : les 4 participants ayant conservé leur identité de hacker ne perçoivent pas de différence entre hacking légal et illégal car, pour eux, le hacking ne caractérise pas un comportement, punissable ou non, mais plutôt un état d'esprit de créativité, de non-conventionnalisme ou de refus d'autorité entre autres comme Steven Levy a déjà pu le décrire en 1984. Ainsi, à l'exception d'un participant, il n'est pas apparu y avoir de regrets, même lorsque ça n'était pas ouvertement indiqué, vers les comportements qu'ils ont pu commettre dans le passé toujours à leur sens portés, si pas par une bonne intention, tout du moins par absence d'intention de nuire. De la même façon, le concept de « cristallisation du mécontentement » décrit par Ray Paternoster & Shawn Bushway (2009) se révèle être inadapté à l'étude du sujet puisque la plupart des participants admet ne pas avoir changé de comportements, mais plutôt de les avoir adaptés à un cadre (légal ou professionnel) mieux décrit.

Finalement, les observations de Judith E. Noordegraaf et Marleen Weunen Kranenbarg (2023) sur l'aspect social des hackers éthiques semblent correspondre aux cercles sociaux décrits par les participants de cette étude : tous ont marqué une importance à avoir une séparation entre amis 'normaux' d'un côté et connaissances liées au hacking de l'autre, d'ailleurs souvent plus fréquentes mais moins familières à cause du contexte du travail qui caractérise leurs rencontres. De la même façon, même les participants les plus proches d'un groupe de pairs déviants dans leur jeunesse s'en sont séparés et tous indiquent une rupture de contact avec des hackers illégaux ou tout du moins un contact très superficiel lors de rencontres en évènements. Ainsi, il semble difficile de confirmer l'hypothèse selon laquelle le hacking légal permettrait de renouer des liens prosociaux puisque ces liens ont toujours existé, avec une place importante, dans la vie des participants. De plus, aucun n'a indiqué de quelconque difficulté à se faire accepter en tant que hacker dans la société, relevant même parfois un intérêt particulier à discuter sur le sujet. Cela révèle, en parallèle à l'histoire tourmentée du hacking, présentée plus haut, une distinction forte entre la vision du hacking au niveau législatif et celle de la société, plus positivement valorisée.

2. Implications

Dans un premier temps, les résultats de cette recherche ont montré à quel point l'aspect social était important à la pratique du hacking. Pour rappel, presque tous les participants ont parlé d'une rencontre avec un pair ou une personne externe au hacking qui leur a montré la voie à suivre. A cet effet, il semble d'abord nécessaire de rappeler et d'encourager certaines observations déjà faites par d'autres auteurs : Judith E. Noordegraaf & Marleen Weunen Kranenbarg (2023) indiquaient qu'il était indispensable de créer un programme de sensibilisation aux risques et dangers du hacking pour les jeunes dès l'école secondaire. La plupart des hackers commence à un jeune âge et il semble déterminant de pouvoir leur faire comprendre rapidement les bases de l'éthique à respecter et de leur donner le matériel nécessaire à assouvir leur curiosité et leur envie d'expérience. Ainsi les autrices recommandent également que les cours de technologie en secondaire soient associés à une discussion approfondie des bons comportements à avoir en ligne, voire des dispositions légales, souvent trop floues. De la même façon, il serait intéressant d'offrir à ces jeunes la possibilité au plus vite d'appliquer leurs compétences dans un cadre plus professionnel en créant une option scolaire dédiée à l'apprentissage technologique, comme cela est déjà le cas pour des matières plus communes telles que les sciences, les maths, ou l'économie.

En dehors du contexte scolaire, il paraît important de continuer à développer des outils permettant aux apprentis hackers à se former sans causer de dommages. Aujourd'hui, de plus en plus de sites sont dédiés à l'apprentissage de façon ludique notamment par l'utilisation de défis *Capture The Flag* dont l'objectif

est d'atteindre un 'drapeau' dissimulé à l'intérieur d'un système informatique souvent en utilisant des méthodes créatives pour y pénétrer. Ces systèmes semblent être un bon compromis entre l'état d'esprit de créativité ou d'inventivité lié au hacking et un cadre sécurisé qui permet de pratiquer sans conséquences. Il convient aussi de faire référence ici à la plateforme grecque HackTheBox qui est née en 2017 et qui permet justement à ses utilisateurs (tant des personnes isolées que des écoles) d'apprendre tout en pratiquant de façon ludique et sécurisée. Il est primordial que ce type d'initiatives continue de se développer dans le futur pour atteindre le plus de personnes possibles, pour les sensibiliser aux dangers des vulnérabilités non réparées et leur permettre de vivre de leur passion dans un environnement satisfaisant tant pour eux que pour la société.

Il est utile de rappeler aussi, comme le faisaient déjà Mario Silic & Paul Benjamin Lowry en 2019, l'importance des hackers expérimentés dans cette sensibilisation qui pourraient servir d'intermédiaires entre la société et les jeunes hackers afin de leur expliquer les potentielles conséquences de hacks paraissant bénins. Le cyberespace dans lequel le hacking prend place empêche parfois d'être conscient des personnes derrière les réseaux, laissant une impression de crime sans visage, or, il est indispensable de faire comprendre que les conséquences, même si elles ne sont pas toujours financièrement importantes, peuvent mener à des conséquences humaines terribles dans certains cas. En réalité, certains participants rencontrés admettaient ne pas en avoir eu conscience quand ils étaient jeunes et souhaitaient aujourd'hui transmettre leurs valeurs et leur histoire à un public plus jeune. Au vu de cette demande, il paraît réalisable d'organiser des rencontres ponctuelles dans des écoles ou dans des évènements rassemblant des groupes de hackers, de faire appel à ces professionnels qui vivent de leur passion pour donner l'exemple.

Dans un second temps, il semble intéressant de s'intéresser de plus près aux collaborations possibles entre hackers et organes de sécurité publique. Il est apparu lors d'une rencontre de préparation à cette recherche que la police, belge en tout cas, collaborait relativement peu souvent avec des hackers repentis par peur qu'ils trahissent la confiance qui leur est confiée, qu'ils ne suivent pas le cadre pratique ou tout simplement qu'ils ne partent ailleurs pour un meilleur salaire. Or, l'appel ponctuel à des hackers externes pourrait mener à une amélioration des compétences dans la recherche d'infractions ou de suspects tout en permettant un allègement de la charge de travail des policiers travaillant dans ce domaine. Cette étude montre d'ailleurs que les hackers qui se sont tournés vers la légalité sont avant tout poussés par un désir de rendre les systèmes informatiques plus sécurisés ou de bénéficier aux autres et que l'argent n'est pas un objectif tant qu'ils peuvent faire ce qu'ils aiment. En ce sens, il apparaît qu'une collaboration n'est pas impensable. Néanmoins, il convient d'indiquer que les hackers sont généralement portés par une appréhension du monde hiérarchique et administratif, ce qui pourrait incapaciter cette participation ou mener à des adaptations. Pour ces raisons, il serait intéressant de mener de futures études sur la potentialité de cette collaboration.

Dans un troisième temps, il avait déjà été indiqué dans l'état de l'art que la terminologie employée dans le domaine du hacking était trop floue et les résultats semblent aller dans le même sens ; plusieurs participants ont marqué le fait qu'il n'y avait pas de distinction entre hacking légal ou illégal, éthique ou non éthique. Il est alors déterminant d'ouvrir la discussion sur les termes à utiliser dans la recherche car la transmission et le partage de connaissances ne peuvent fonctionner si les termes utilisés énoncent une définition différente pour chacun. Il est important de reconnaître le hacking pour ce qu'il est : un état d'esprit, une manière d'être caractérisée, entre autres, par une inventivité, une liberté et une volonté de transmettre. Ainsi, tous les hackers ne sont pas forcément légaux ou illégaux et tous les experts en cybersecurité ne sont pas forcément des hackers. Un participant le rappelle d'ailleurs de façon amusante en indiquant, à la manière de Richard Barber : « *Personne ne se dit pharmacien éthique parce qu'il ne vend pas de substances illégales* ». A cet effet, il pourrait être intéressant d'envisager une revue systématique de littérature reprenant les différents termes et définitions utilisées dans les différents articles sur le sujet. En attendant, il convient d'apporter quelques éléments de réponses à cette

problématique afin d'appeler à une mise en commun des avis multiples des experts du domaine. Une première possibilité serait, comme le proposaient certains participants, de ne distinguer le légal de l'illégal que par l'appellation de crime ou non, ce serait par exemple le cas du piratage, du vol de données ou du faux informatique. Dans ce cas, chaque infraction serait étudiée de façon plus spécifique et isolée, ce qui serait alors perdu en généralisabilité serait gagné avec un approfondissement des différences de particularités possibles entre ces différents auteurs, notamment dans le cadre des motivations qui les pousse à agir. Une autre solution pourrait être de remettre en avant l'utilisation du terme 'cracker' qui représenterait un hacker mû par de mauvaises intentions, par opposition au hacker qui serait alors mû par de bonnes intentions. Dans ce cas, il pourrait être problématique néanmoins de classer certaines activités comme le hacktivisme, dont l'intention peut sembler bonne ou mauvaise selon le camp choisi. Une dernière possibilité envisagée serait d'utiliser la terminologie de *white, grey et black hat* hackers, son avantage est d'être assez facilement comprise, néanmoins, elle perd beaucoup en spécificité et nécessiterait un encadrement plus strict pour déterminer ce qui est caractérisé comme un comportement qui rentre dans l'une ou l'autre de ces catégories. Encore une fois, ces propositions ne sont pas exhaustives et n'ont pas pour objectif d'imposer un choix mais plutôt d'ouvrir un débat vers un consensus scientifique.

Finalement, il convient de terminer sur certaines implications légales en revenant sur l'article 2 de la Convention sur la Cybercriminalité de 2001. Pour rappel, celui-ci traite de 'l'accès illégal' (il est d'ailleurs intéressant de remarquer au regard du paragraphe précédent que l'article n'utilise pas le terme de 'hacking') et le définit comme : « *l'accès intentionnel et sans droit à tout ou partie d'un système informatique* ». Au sens des résultats analysés, il semble que l'intentionnalité générale qui est prévue soit un élément moral trop large et englobant ainsi nombre de hackers motivés par des intentions bénéfiques à la protection des systèmes. Ainsi, comme certains participants l'indiquaient, la réelle différence entre un comportement de hacker légal ou illégal est l'intention portée derrière le geste. Dans ce sens, il semble qu'il serait plus conforme à la réalité de punir l'accès illégal uniquement s'il est porté par une volonté de nuire ou une volonté frauduleuse puisque, même si la loi se doit d'être dissuasive, il serait dommageable de dissuader certains hackers bien intentionnés de trouver des failles de sécurité avec la seule volonté de les réparer. Il est important de préciser que, si la convention se veut liante aux états l'ayant signée et ratifiée, elle donne la possibilité dans le même article 2 de caractériser la définition de l'accès illégal comme : « *commis en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou* ***dans une autre intention délictueuse****, ou soit en relation avec un système informatique connecté à un autre système informatique* ». Il est donc totalement envisageable, au niveau national, d'inclure une nécessité d'intention de nuire pour que le comportement soit puni.

Dans la partie d'état de l'art, une cause de justification liée à la divulgation coordonnée de vulnérabilités a été introduite brièvement et pourrait sembler être une bonne solution à ce manque légal, déjà disponible dans certains pays comme la Belgique. Néanmoins, il reste étonnant que cette cause, amenée par la directive NIS 2, soit toujours considérée comme une exception à la règle et non comme la règle en tant que telle. En effet, il apparaît que les motivations présentes chez les participants au moment de commettre certains comportements illégaux étaient avant tout la curiosité ou la volonté de rendre compte de dangers. A nouveau, il n'apparaît pas, dans ces cas, que leurs comportements étaient dangereux ou aient justifié une peine. A l'inverse, il pourrait même sembler que ces attitudes soient favorables à la création de systèmes technologiques mieux sécurisés.

Pour les mêmes raisons, des *Computer Emergency Response Team* (C.E.R.T.) avaient été mis en place pour permettre aux hackers d'avoir une plateforme servant d'intermédiaire avec les entreprises et ainsi faciliter les discussions mais aussi protéger les hackers détenant des preuves d'une vulnérabilité découverte. Malgré ces efforts, il semble, aux dires des participants, encore parfois compliqué de communiquer avec les sociétés, certaines étant toujours peu à même d'admettre les failles de leur système ou de mettre en place les efforts pour les réparer. Certains indiquent même une forme d'injustice

légale dans le rapport hacker – entreprise : même si des pénalités existent au regard du Règlement Général de Protection des Données pour les entreprises, certaines continuent d'ignorer volontairement les avertissements et les rapports de vulnérabilité, mettant alors en danger la protection des données de leurs utilisateurs. Dans ces cas, les personnes rencontrées se sont dit tiraillées entre l'idée de publier les résultats sans accord de l'entreprise et celle de garder les informations pour eux, parfois même ils ont hésité à contacter le C.E.R.T. ou l'entreprise concernée par peur des conséquences. Il est alors important de continuer à appuyer sur l'importance pour les entreprises de sécuriser leurs systèmes notamment en jouant sur le coût de l'inaction (Pralle, S. B., 2009).

Ces 3 raisons mises ensemble semblent indiquer qu'il existe aujourd'hui un risque que la loi et les mesures mises en place amènent un hacker en possession d'informations, parfois critiques, à les garder pour lui plutôt qu'à les partager avec l'entreprise ou la société par crainte d'être puni légalement. Caractériser ces comportements mus par une volonté de sécurisation des systèmes informatiques derrière une illégalité justifiée porte le risque de préférer l'effet de la dissuasion à la criminalité plutôt que la valorisation des comportements bénéfiques à une meilleure protection de données. Or, la société étant de plus en plus imprégnée de la technologie, il semble indispensable qu'elle se munisse de toute protection disponible pour sécuriser les informations qu'elle y partage. En ce sens, il convient de renverser la tendance en rendant à ces comportements leur légalité pleine et en excluant, par exception, les intrusions mal intentionnées.

3. Limitations de l'étude

Comme toute recherche en sciences humaines, cette étude n'est pas exempte de certaines limites. La première est liée à son design qualitatif et au nombre de participants compris dans l'échantillon. Les études qualitatives sont rarement utilisées pour généraliser des résultats mais plutôt pour décrire des voies d'explications de phénomènes pour de futures études. Néanmoins, n'avoir pu rencontrer que 5 participants reste décevant d'un point de vue méthodologique : effectivement, il s'est avéré lors de la phase de recrutement que la population recherchée était difficile d'accès, soit parce qu'une collaboration ne les intéressait pas, notamment par manque de compensation pécuniaire, soit parce qu'il est tabou et dangereux d'avouer des actes illégaux qui pourraient entraver leur vie professionnelle à un inconnu dans le cadre d'une rencontre. Malgré la volonté de flexibilité et les différentes adaptations mises en place, comme la possibilité d'*e-interview*, peu de personnes semblaient intéressées. Une solution qui aurait pu être mise en place est l'appel aux participants à différer l'information autour d'eux, cependant, par crainte de réduire le nombre d'intéressés avec cette demande, il a semblé préférable de s'en tenir à l'analyse détaillée de ces 5 participants. Il est cependant apparu que les résultats observés dans cet échantillon se rapprochaient de résultats d'autres études précédentes, ce qui pourrait signifier que l'échantillon est représentatif, même s'il est préjudiciable de l'affirmer à ce niveau. Pour éviter ce biais, il est indispensable que de futures recherches viennent à confirmer ou infirmer ces résultats par réplication sur un plus grand nombre de hackers.

Une seconde limite réside encore dans l'échantillon présenté dans cette recherche : il est possible que les participants ayant accepté la rencontre l'aient fait parce qu'ils avaient atteint un stade de désistance plus abouti. Il n'est malheureusement pas possible de confirmer cette hypothèse mais il serait intéressant de chercher à atteindre des populations de hackers occupant un poste légal mais qui continueraient à avoir des comportements illégaux dans de futures études. Cependant, si les hackers repentis étaient difficiles d'accès, les hackers qui continuent d'avoir une activité illégale, s'ils existent, devraient être encore plus inaccessibles par crainte que leur anonymat soit entravé et que leurs comportements puissent être dévoilés à leurs employeurs.

Finalement, une dernière limite potentielle concerne le concept de désirabilité sociale qui caractérise une tendance du participant à vouloir se décrire selon une image plus favorable (McCrae, R. R. & Costa, P. T., 1983). Il est possible que certaines des personnes rencontrées aient voulu paraître plus conformes qu'ils ne le sont dans la réalité en dissimulant certains comportements ou en mettant en avant des

motivations plus conventionnelles que d'autres. Toutefois, il faut rappeler que les hackers se caractérisent par une non-conformisation à la société et que les participants mettaient en avant qu'il était moins nécessaire pour eux de chercher la validation externe. De plus, lors des entretiens par visioconférence (il est difficile de le déterminer pour les *e-interviews*), les participants n'ont pas semblé vouloir dissimuler quoi que ce soit, ils ont pu parfois rentrer dans certains détails supplémentaires à ce qui leur était demandé et ils semblaient répondre de façon naturelle. Toutes ces raisons font qu'il paraît improbable que ce phénomène ait eu un effet sur les résultats de cette recherche.

Conclusion

L'objectif de cette recherche était de mieux rendre compte des motivations des hackers à se tourner vers la légalité et à la pertinence du hacking légal comme vecteur de désistance et ainsi combler le manque de recherches sur ce sujet. Pour y parvenir, des hackers avec une expérience illégale ayant rejoint des postes légaux ont été rencontrés afin d'expliquer leur trajectoire et de revenir sur les moments importants qui ont influencé ce choix. Les résultats obtenus et mis en lumière au travers de la théorie de la transformation cognitive de Giordano & al. (2002) ont semblé infirmer l'hypothèse que le métier pourrait servir de levier pour la désistance, favorisant plutôt les théories de la maturation, indiquant que l'attrait pour l'illégalité disparaît avec l'âge et la sagesse, ou celles de l'apprentissage social puisque les histoires rencontrées étaient parsemées de rencontres importantes dans le changement de trajectoire vers la légalité dans la vie des participants.

L'analyse des résultats a permis d'insister sur l'intérêt d'encadrer la jeunesse dans les premières expériences qu'elle rencontre avec le monde du hacking et d'encourager la transmission d'expériences illégales de hackers avérés plutôt que leur dissimulation ainsi que d'envisager des changements légaux pour mieux s'adapter aux réalités décrites par les participants. Il est indispensable que la société comprenne qu'il est préjudiciable de condamner un hacker pour ce qu'il est et de lui fermer des opportunités de futur professionnel plutôt que de lui donner les clefs pour se réintégrer et lui apprendre à utiliser ses connaissances à bon escient. Il convient de mettre en avant la valorisation de la protection des systèmes plutôt que son entrave.

Cette recherche a permis de rappeler que le hacking, comme le montrait déjà son histoire, est toujours empreint de créativité et de volonté de repousser les limites des technologies actuelles pour bénéficier à la société et non pour y nuire. Elle a aussi pu permettre de se poser la question de la pertinence de l'étude du 'hacking illégal' sous ces termes et révélé l'importance pour les chercheurs de se mettre d'accord sur les termes et les définitions utilisées pour décrire les phénomènes étudiés. Le hacking est aujourd'hui encore trop peu recherché dans son aspect criminologique, par rapport à son aspect technologique. Cette étude a tenté de montrer ce que la criminologie pouvait apporter à ce champ de recherche en remettant l'humain au centre et souhaite rappeler qu'une intrusion informatique n'est pas qu'une affaire d'ordinateurs ou d'autres appareils, mais avant tout l'affaire de deux êtres humains de chaque côté de cet intermédiaire.

Au travers de ces observations, ce travail veut finalement rendre compte d'un mécanisme de défense précipité trop souvent mobilisé face à la peur que la méconnaissance du monde technologique recouvre. Foucault écrivait, il y a presque 50 ans, 'surveiller et punir', la formulation semble aujourd'hui adaptée à la façon dont le monde législatif regarde le hacking de loin, tentant de le condamner plutôt que d'aller à sa découverte. Ainsi, une dernière question se pose : « n'est-il pas temps de rétablir l'ordre des choses en se demandant 'faut-il punir ?' plutôt que 'comment punir ?' ».

Bibliographie

Bampton, R., Cowton, C., & Downs, Y. (2013). The E-Interview in Qualitative Research. In *IGI Global eBooks* (pp. 329–343). https://doi.org/10.4018/978-1-4666-3918-8.ch019

Barber, R. (2001). Hackers profiled – Who are they and what are their motivations? *Computer Fraud & Security, 2001*(2), 14-17. https://doi.org/10.1016/s1361-3723(01)02017-6

Bikeev, I.I., Kabanov, P., Begishev, I.R., & Khisamova, Z.I. (2019). Criminological risks and legal aspects of artificial intelligence implementation. *International Conferences on Artificial Intelligence, Information Processing and Cloud Computing*.

Blauth, T. F., Gstrein, O. J., & Zwitter, A. (2022). Artificial Intelligence Crime: An overview of Malicious use and abuse of AI. *IEEE Access, 10,* 77110-77122. https://doi.org/10.1109/access.2022.3191790

Boyatzis, R. E. (1998). *Transforming qualitative information: Thematic Analysis and Code Development*. SAGE.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brown, C. (2015). White or Black Hat? An Economic Analysis of Computer Hacking.

Bugcrowd (2021). Inside the mind of a hacker. Retrieved from https://www.bugcrowd.com/resources/guides/inside-the-mind-of-a-hacker/

Chang, L. Y., & Whitehead, J. R. (2021). What the hack: Reconsidering responses to hacking. *Asian Journal of Criminology*, *17*(2), 113–126. https://doi.org/10.1007/s11417-021-09356-1

Chng, S., Lü, H., Kumar, A., & Yau, D. K. Y. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*, *5*, 100167. https://doi.org/10.1016/j.chbr.2022.100167

Choi, KS., Lee, C.S. & Louderback, E.R. (2020). Historical Evolutions of Cybercrime: From Computer Crime to Cybercrime. In: Holt, T., Bossler, A. (eds). The Palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-784412

Clarke, R. et Cornish, D. (1985). Modeling Offenders' Decisions: A Framework for Research and Policy. Crime and Justice (Chicago, Ill.), 6, 147–185. https://doi.org/10.1086/449106

Convention de Budapest sur la Cybercriminalité. Disponible sur [Council of Europe – Convention on Cybercrime (ETS No. 185) – Translations - Treaty Office (coe.int)]

DeJarvis Oliver & Adriane. B. Randolph (2022) Hacker Definitions in Information Systems Research, Journal of Computer Information Systems, 62:2, 397-409, https://doi.org/10.1080/08874417.2020.1833379

Del-Real, C., & Rodriguez Mesa, M.J. (2022). From black to white: the regulation of ethical hacking in Spain. *Information & Communications Technology Law, 32*, 207 - 239.

Dennin, D. E. (2011). Cyber Conflict as an Emergent Social Phenomenon, Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications (T. J. Holt and B. Schell eds.), IGI. http://hdl.handle.net/10945/37158

Furnell, S. (2002). *Cybercrime: Vandalizing the Information Society*. Addison-Wesley Professional.

Gillespie, A.A. (2019). Cybercrime: Key Issues and Debates (2nd ed.). Routledge. https://doi.org/10.4324/9781351010283

Giordano, P.C., Cernkovich, S.A., & Rudolph, J.L. (2002). Gender, Crime, and Desistance: Toward a Theory of Cognitive Transformation. *American Journal of Sociology, 107*, 990 - 1064.

Grabosky, P. N., Smith, R. G., & Wright, P. (1998). *Crime in the digital age: Controlling telecommunications and cyberspace illegalities*. Carfax Publishing, Taylor and Francis Group. https://doi.org/10.4324/9780203794401

HackerOne (2021). The 2021 hacker report. Retrieved from https://www.hackerone.com/resources/reporting/the-2021-hacker-report

Hayward, K. J., & Maas, M. M. (2021). Artificial intelligence and crime: A primer for criminologists. *Crime, Media, Culture*, *17*(2), 209-233. https://doi.org/10.1177/1741659020917434

Hirschi, T., & Gottfredson, M. R. (1983). Age and the Explanation of Crime. *American Journal of Sociology*, *89*(3), 552–584. https://doi.org/10.1086/227905

Holt, T. J. (2020). Computer Hacking and the Hacker Subculture. In: Holt, T. J., & Bossler, A. (eds). The palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-78440-3_31

Hughes, E. C. (1945). *Dilemmas and contradictions of status*.

Interpol. (2022). *2022 Interpol Global Crime Trend Summary Report. https://www.interpol.int/en/content/download/18350/file/Global%20Crime%20Trend%20Summary%20Report%20EN.pdf*

Jacquet-Chiffelle, DO., Loi, M. (2020). Ethical and Unethical Hacking. In: Christen, M., Gordijn, B., Loi, M. (eds). The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology, vol 21. Springer, Cham. https://doi.org/10.1007/978-3-030-29053-5_9

Jordan, T., & Taylor, P. H. (1998). A Sociology of Hackers. *The Sociological Review*, *46*(4), 757–780. https://doi.org/10.1111/1467-954x.00139

Katz, J. (1988). *Seduction Of Crime*.

Lastdrager, E.E. Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Sci* **3**, 9 (2014). https://doi.org/10.1186/s40163-014-0009-y

Levy, S. (2010). *Hackers: Heroes of the Computer Revolution - 25th Anniversary Edition*. O'Reilly Media.

Loggen, J. & Moneva, A. & Leukfeldt, E.. (2023). *Pathways into, desistance from, and risk factors related to cyber-dependent crime: A systematic narrative review*. [preprint] https://doi.org/10.31219/osf.io/kpfrb.

Mahmud, A. (2023). Application and Criminalization of Artificial Intelligence in the Digital Society: Security Threats and the Regulatory Challenges. *Journal of Applied Security Research*, *18*(1), 1–15. https://doi.org/10.1080/19361610.2021.1947113

Maimon, D., & Louderback, E. R. (2019). Cyber-Dependent Crimes: An Interdisciplinary Review. *Annual Review of Criminology*, *2*(1), 191–216. https://doi.org/10.1146/annurev-criminol-032317-092057

Maruna, S., & Farrall, S. (2004). Desistance from Crime: A Theoretical Reformulation. *Kölner Zeitschrift Für Soziologie Und Sozialpsychologie*, 171–194. https://doi.org/10.1007/978-3-322-80474-7_7

Maurushat, A. (2019). *Ethical Hacking*. University of Ottawa Press.

McCrae, R. R., & Costa, P. T. (1983). Social desirability scales: More substance than style. *Journal of Consulting and Clinical Psychology*, *51*(6), 882–888. https://doi.org/10.1037/0022-006x.51.6.882

McNeill, F. (2016). Desistance and criminal justice in Scotland. In H. Croall, G. Mooney, & M. Munro (Eds.), Crime, justice and society in Scotland (pp. 200–216). London: Routledge

Nehls, K., Smith, B. D., & Schneider, H. A. (2015). Video-Conferencing interviews in qualitative research. In *Advances in knowledge acquisition, transfer, and management book series/Advances in knowledge acquisition, transfer and management book series* (pp. 140 - 157). https://doi.org/10.4018/978-1-4666-6493-7.ch006

Nicholson, S. (2019). How ethical hacking can protect organisations from a greater threat. *Computer Fraud & Security*, *2019*(5), 15–19. https://doi.org/10.1016/s1361-3723(19)30054-5

Noordegraaf, J.E., & Weulen Kranenbarg, M. (2023). Why do young people start and continue with ethical hacking? A qualitative study on individual and social aspects in the lives of ethical hackers. *Criminology & Public Policy*.

Nugent, B., & Schinkel, M. (2016). The pains of desistance. Criminology and Criminal Justice, 16(5), 568– 584

Oreku, G. S., Mtenzi, F. J. (2017). Cybercrime: Concerns, Challenges and Opportunities. In: Alsmadi, I., Karabatis, G., Aleroud, A. (eds). Information Fusion for Cyber-Security Analytics. Studies in Computational Intelligence, vol. 691, Springer, Cham. https://doi.org/10.1007/978-3-319-44257-0 6

Palmieri, M. J., Shortland, N., & McGarry, P. (2021). Personality and online deviance: The role of reinforcement sensitivity theory in cybercrime. *Computers in Human Behavior*, *120*, 106745. https://doi.org/10.1016/j.chb.2021.106745

Paquet-Clouston, M., Haslhofer, B., & Dupont, B. (2019). Ransomware payments in the Bitcoin ecosystem. *Journal of Cybersecurity*, *5*(1). https://doi.org/10.1093/cybsec/tyz003

Paternoster, R., & Bushway, S. D. (2009). Desistance and the "Feared Self": toward an identity theory of criminal desistance. *Journal of Criminal Law & Criminology, 99*(4), 1103-1156. https://dialnet.unirioja.es/servlet/articulo?codigo=3752580

Pralle, S. B. (2009) Agenda-setting and climate change, *Environmental Politics*, 18:5, 781-799. https://doi.org/10.1080/09644010903157115

Sampson, Robert J., and John H. Laub. 1993. *Crime in the making: Pathways and turning points through life*. Cambridge, MA: Harvard Univ. Press.

Schwab, K. (2017). *The Fourth Industrial Revolution*. Penguin UK.

Silic, M., & Lowry, P. B. (2019). Breaking Bad in Cyberspace: Understanding why and how Black Hat Hackers Manage their Nerves to Commit their Virtual Crimes. *Information Systems Frontiers*, *23*(2), 329–341. https://doi.org/10.1007/s10796-019-09949-3

Skarðhamar, T., & Savolainen, J. (2014). Changes in Criminal Offending Around the time of Job Entry: A Study of Employment and Desistance. *Criminology, 52*(2), 263-291. https://doi.org/10.1111/1745-9125.12037

Statista. (September 14, 2023). Estimated cost of cybercrime worldwide 2017-2018 (in trillion U.S. dollars) [Graph]. In *Statista*. Retrieved November 21, 2023, from https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide

Steinmetz, K. F. (2015). CRAFT(Y)NESS: An Ethnographic Study of Hacking. *The British Journal of Criminology*, *55*(1), 125–145. http://www.jstor.org/stable/43819263

Taylor, P. A. (1999). *Hackers: Crime and the digital Sublime*. http://ci.nii.ac.jp/ncid/BA44876451

The Mentor (1986). The Conscience of a Hacker. *Phrack, Volume one (7).*

Turgeman-Goldschmidt, O. (2008). Meanings that Hackers Assign to their Being a Hacker. *International Journal of Cyber Criminology, 2*(2), 382. https://www.cybercrimejournal.com/Orlyijccdec2008.pdf

Turkle, S. (1984). *The second self: Computers and the Human Spirit*. Touchstone.

Van Beveren, J. (2001). A Conceptual Model of Hacker Development and Motivations. *Journal of E-Business*, *Vol. 1*(Issue 2). http://www.dvara.net/HK/beveren.pdf

Weulen Kranenbarg, M. (2019). Contrasting cyber-dependent and traditional offenders. A comparison on criminological explanations and potential prevention methods. In: Leukfeldt, R. & Holt, T. J. (2019b). *The human factor of cybercrime.* https://doi.org/10.4324/9780429460593

Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and Society*. SAGE.

Zand, E. van 't, Matthijsse, S., Fischer, T., & Wagen, W. van der. (2021). Interventions for cyber offenders. In J. J. Oerlemans & M. Weulen Kranenbarg (Eds.), Essentials in cybercrime. A criminological overview for education and practice (pp. 255-283). The Hague: Eleven. Retrieved from https://hdl.handle.net/1887/3307593