Criminologie, Forensique et Sécurité

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

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

Article de recherche

Criminologie, Forensique et Sécurité

2023 | 1 (1) : 3481

https://doi.org/10.26034/la.cfs.2023.3481

Licence : Creative Commons 4.0

Sous-culture pédophile et processus d'enculturation en matière de cybersécurité: une analyse en classes latentes des thématiques sécuritaires sur le dark web

Julien Chopin[1,2,3], David Décary-Hétu[1], Emmanuelle Marois[1], Léanne Vincendon[1]

[1] Centre International de Criminologie Comparée, Université de Montréal
[2] Terrorism, Violence and Security Institute Research Centre, Simon Fraser University
[3] Ecole de Travail Social et de Criminologie, Université de Laval

Contact: julien.chopin@umontreal.ca

Résumé

L'échange et l'acquisition de compétences de cybersécurité sur le dark web par la communauté pédophile font partis de la sous-culture pédophile sur Internet. Dans cette perspective, cette étude s'intéresse au processus d'enculturation en matière de cybersécurité par les utilisateurs de forums pédophiles sur le dark web et est encadrée par l'approche de l'expertise criminelle. Spécifiquement, cette recherche a pour objectif de déterminer si les thématiques discutées constituent un ensemble homogène ou hétérogène et si elles sont associées à des indicateurs d'expertise et d'intérêt de la part de la communauté pédophile. Cette étude se fonde sur l'analyse de 290 fils de discussion (FDDs) spécifiquement dévolus aux sujets de cybersécurité, extrait de trois forums pédophiles sur le dark web. Une analyse en classes latentes a permis de classifier les différents FDDs en quatre classes en fonction des thématiques traitées : stratégies réactives de confrontation avec la justice, stratégies proactives basiques, stratégies de lutte contre les menaces non judiciarisées, stratégies proactives avancées. Les indicateurs de validité externes permettent de confirmer l'existence d'un lien entre les sujets traités, le niveau d'expertise et le niveau d'intérêt des utilisateurs de ces forums confirmant l'existence d'un processus d'enculturation au sein de la sous-culture pédophile sur internet.

Mots clés :

Expertise criminelle, sous-culture pédophile, enculturation, stratégies de protection, cybersécurité, Dark web

Pedophile subculture and enculturation processes in cybersecurity: a latent class analysis of security themes on the dark web

Abstract

The exchange and acquisition of cyber security skills on the dark web by the pedophile community are part of the pedophile subculture on the Internet. In this perspective, this study focuses on the process of enculturation about cyber security by dark web pedophile forum users, framed by the approach of criminal expertise. Specifically, this research aims to determine whether the topics discussed constitute a homogeneous or heterogeneous set and whether they are associated with indicators of expertise and interest from the pedophile community. This study is based on the analysis of 290 threads specifically devoted to cybersecurity topics, extracted from three pedophile forums on the dark web. A latent class analysis allowed to classify the different threads into four classes according to the topics discussed: reactive strategies of confrontation with justice, basic proactive strategies, counter strategies against non-judicial threats, advanced proactive strategies. The external validity indicators confirm the existence of a link between the topics covered, the level of expertise and the level of interest of the users of these forums, confirming the existence of an enculturation process within the pedophile subculture on the Internet.

Keywords :

Criminal expertise, pedophile subculture, enculturation, protection strategies, cybersecurity, Dark web

Citation : Chopin, J., Décary-Hétu, D., Marois, E., Vincendon, L. (2023) Sous-culture pédophile et processus d'enculturation en matière de cybersécurité: une analyse en classes latentes des thématiques sécuritaires sur le dark web *Criminologie, Forensique et Sécurité*, 1 (1) : 3481.

© Julien Chopin, David Décary-Hétu, Emmanuelle Marois, Léanne Vincendon, 2023

Introduction

La criminalité commise en ligne est en plein essor et contribue au développement de nouvelles brèches pour les individus s'engageant dans la criminalité (Caneppele et Aebi, 2019; Levi, 2017; Linde et Aebi, 2020). L'évolution des espaces virtuels a permis l'émergence d'environnements propices aux échanges, contribuant au renforcement des croyances et au développement des compétences criminelles. Ce phénomène connu sous le terme de processus d'enculturation a été particulièrement observé au sein de la communauté pédophile[1] (c.-à-d. les individus manifestant un intérêt sexuel envers les enfants) et a conduit à l'identification d'une sous-culture pédophile en ligne (Holt et al., 2010). La perspective de la sous-culture en criminologie et sociologie désigne des groupes d'individus dont les valeurs, les normes, les traditions et les rituels sont en désaccord avec la culture dominante (Brake, 1980; Young, 2010). Dans ce contexte, les individus faisant partie de ces entités transmettent, apprennent et échangent en lien avec les différentes composantes qui définissent la sous-culture en question (Young, 2010). Les environnements virtuels qui existent offrent aux individus une opportunité de se réunir dans un espace commun pour discuter et trouver du support à leurs fantaisies sexuelles (Durkin et Bryant, 1999; Jenkins, 2001) ainsi qu'à échanger et distribuer du matériel d'exploitation sexuel d'enfants (Durkin, 1997; Fontana-Rosa, 2001; Fortin, 2014; Holt et al., 2010). Au-delà des aspects sexuels, les questions sécuritaires trouvent un intérêt tout particulier auprès de la communauté pédophile qui cherche à se prémunir contre les menaces extérieures, dont la détection par la police (Holt et al., 2010; Paquette et Fortin, 2021). L'intérêt et la capacité des individus à se prémunir contre les menaces extérieures sont des composantes clés de l'approche du choix rationnel qui assument que les individus prennent des décisions afin de compléter leur crime avec succès tout en évitant les risques y étant inhérents (Cornish et Clarke, 1986). L'acquisition et l'échange d'informations relatives à la cybersécurité et à la capacité des individus à éviter la détection par les autorités des activités pédophiles en ligne s'inscrit donc dans l'idée que les individus rationalisent leurs processus décisionnels et comportementaux pour éviter les conséquences négatives dont ils pourraient souffrir. Bien que cet aspect soit un sujet d'intérêt prépondérant pour la communauté pédophile (Holt et al., 2010), l'utilisation de stratégies pour se prémunir contre les risques par les individus associés à des crimes sexuels en ligne a été très peu étudiée. Dépendamment du type d'échantillon analysé, la prévalence d'utilisation de telles stratégies varie entre 5 % et 80 % des individus (Paquette et Fortin, 2021; Seto et al., 2010; Steel et al., 2020). Cette étude propose ainsi d'étendre les connaissances sur le sujet en analysant la thématique de la cybersécurité des utilisateurs de forums pédophiles dans un contexte de sous-culture pédophile et d'enculturation. Concrètement, l'objectif consiste à analyser les contenus spécialisés afin d'identifier des schémas particuliers de connaissances, d'intérêts pour la communauté et de niveau d'expertise.

Choix rationnel, expertise criminelle et crimes sexuels commis dans un espace virtuel

L'approche du choix rationnel offre un cadre théorique pour analyser et comprendre les comportements adoptés et les décisions prises par les individus dans un contexte criminel. Le postulat de base de cette approche suggère que les individus opèrent une analyse coût-bénéfice des situations afin d'influencer leur processus décisionnel et comportemental (Cornish et Clarke, 1986; Cornish et Clarke, 1987; Cornish et Clarke, 2008). Cette analyse s'effectue à un niveau macro-analytique avec la décision pour un individu de s'engager ou non dans une activité criminelle, mais également à un niveau micro-analytique en influençant la succession de décisions et de comportements que l'individu doit adopter tout au long du processus criminel pour mener à bien son action (Cornish et Clarke, 1986). L'analyse coût-bénéfice des individus les conduits à s'interroger sur deux concepts : 1) leur capacité à commettre avec succès le crime dans lequel il s'engage (p. ex. parvenir à dérober un bien avec une valeur significative) et 2) à éviter les menaces extérieures (p. ex. éviter la détection policière ou l'intervention d'un tiers) (Chopin, Paquette et Beauregard, 2022; Nee, 2015; Nee et Taylor, 2000). Le second concept, relatif à la gestion des menaces extérieures, est éminemment plus transversal, car moins dépendant du type de crime et de la motivation des individus, et a été théorisé sous la notion d'expertise criminelle. L'idée sous-jacente consiste à considérer que de la même manière que dans des contextes non criminels (Ericsson et al., 2018), les individus s'impliquant dans une activité délinquante présentent un niveau de capacité et de compétence leur permettant la mise en œuvre de stratégies pour tenter d'éviter les menaces extérieures (Nee et Ward, 2015; Ward, 1999). Cette hypothèse théorique discutée dès le début du XXe siècle (Sutherland, 1937) a connu un développement notable au début du XXIe siècle avec une multiplication d'études empiriques examinant différents types de crimes (voir p. ex. Cherbonneau et Copes, 2005; Copes et Cherbonneau, 2006; Nee, 2015; Reale et al., 2021a, 2021b; Topalli, 2005; Ward, 1999). Les résultats ont ainsi démontré que les individus impliqués dans une activité criminelle présentaient un continuum de compétences leur permettant de mettre en place des stratégies pour éviter les menaces extérieures et particulièrement l'identification par les forces de police (p. ex. Beauregard et Bouchard, 2010; Chopin, Paquette et Beauregard, 2022; Nee et Meenaghan, 2006; Nee et al., 2015; Reale et al., 2021a, 2021b).

Dans le contexte du débat doctrinal consistant à déterminer l'applicabilité des modèles théoriques initialement façonnés pour les crimes commis dans un contexte hors-ligne à ceux réalisés dans un contexte virtuel, cette approche a été notamment testée dans le cadre des crimes sexuels commis en ligne (c-.à-d. production, échange et consommation de matériel d'exploitation sexuelle d'enfants en ligne ; leurre d'enfants). Bien que marginales, les études ayant porté sur ce sujet ont montré la capacité supérieure de certains individus impliqués dans une criminalité commise dans un espace virtuel à se prémunir contre les menaces extérieures (Chopin, Paquette et Fortin, 2022; Paquette et Fortin, 2021; Seto et al., 2010; Steel et al., 2020; Wolak et al., 2011). Steel et al. (2020)

[1] D'après le DSM (American Psychiatric Association, 2013), la pédophilie réfère au diagnostic d'un trouble de la sexualité caractérisé par des fantasmes et une excitation sexuelle envers un enfant prépubère pendant une durée d'au moins six mois, qu'il y ait ou non passage à l'acte. L'établissement formel de ce diagnostic pour les utilisateurs de forums ayant pour but de faciliter les discussions et de mettre en relation les personnes intéressées par l'établissement de relations romantiques ou affectives avec des enfants n'est pas possible. Cependant, dans la mesure où presque tous les utilisateurs des forums ont déclaré avoir un intérêt sexuel pour les enfants, fantasmer sur eux ou parler de leur excitation il semble approprié de considérer que la population du forum est composée de pédophiles, en particulier ceux qui discutent de relations physiques ou émotionnelles avec des enfants. Par conséquent, les termes de « pédophilie » et de « pédophile » sont utilisés tout au long de cet article (pour plus de détails voir Holt et al., 2010).

© Julien Chopin, David Décary-Hétu, Emmanuelle Marois, Léanne Vincendon, 2023

proposent une revue de la littérature exhaustive sur les techniques utilisées par les consommateurs de matériel d'exploitation sexuel d'enfants. Parmi les principales stratégies utilisées par ces personnes, l'utilisation de Tor, des cryptomonnaies, des systèmes permettant la protection de l'identité des individus échangeant du matériel d'exploitation sexuelle d'enfants (p. ex. Freenet, Usenet), et les services de réseaux privés virtuels (VPN) sont mentionnés (voir p. ex. Acar, 2017; Chohan, 2017; Chopin, Paquette et Fortin, 2022; Loeb, 2017; Owen et Savage, 2015; Paquette et Fortin, 2021; Penna et al., 2005; Steel et al., 2020). En outre, d'autres stratégies telles que le stockage de contenus illégaux sur des dispositifs externes, le cryptage des données et de communications ainsi que des dispositifs spécifiques liés à l'utilisation des téléphones cellulaires sont également mentionnées (Krone et al., 2017; McCarthy, 2010; Paquette et Fortin, 2021; Sanger et Chen, 2014; Steel et al., 2020).

Sous-culture pédophile, enculturation et expertise criminelle

Au-delà de l'identification de l'utilisation de techniques spécifiques par les individus impliqués dans les crimes sexuels commis dans un espace virtuel, l'un des questionnements fondamentaux sur le sujet a consisté à comprendre comment s'opérait cette acquisition de compétences spécifiques. Les études ont suggéré depuis longtemps qu'Internet pouvait représenter un espace privilégié pour les individus présentant des tendances pédophiles afin d'échanger sur leurs intérêts sexuels, leurs techniques pour identifier des cibles, pour transmettre du matériel d'exploitation sexuel d'enfants, ou encore trouver du support à leurs fantaisies sexuelles et comportements (Durkin, 1997; Durkin et Bryant, 1999; Fontana-Rosa, 2001; Jenkins, 2001; Quayle et Taylor, 2002; Taylor et al., 2001; Wolak et al., 2005; Wolak et al., 2003). Dans une recherche considérée comme un précurseur dans le domaine, Holt et al. (2010) réalisent une analyse qualitative du contenu de cinq forums pédophiles. Leurs résultats soutiennent l'existence d'une sous-culture[2] pédophile en ligne à travers laquelle les individus échangent des informations. Les quatre thèmes de cette sous-culture sont : la marginalisation, la sexualité, les aspects légaux, et la sécurité contre les menaces extérieures (Holt et al., 2010). Il est intéressant de constater que les aspects sécuritaires et légaux représentent la moitié des composantes de la sous-culture pédophile. Les résultats de Holt et al. (2010) suggèrent clairement la possibilité d'un processus d'enculturation conduisant à l'acquisition de compétences et au renforcement des croyances. Dans une étude plus récente, Chopin, Paquette et Fortin (2022) s'intéressent aux schémas d'acquisition de compétences des individus impliqués dans des crimes sexuels en ligne. À partir d'une analyse de réseau de neurones artificiels, ils identifient deux schémas principaux d'acquisition de compétences : 1) l'existence de connaissances préalables (p. ex. acquise durant des études, par les pairs, etc.), 2) l'apprentissage par la confrontation avec le système judiciaire. Ce dernier schéma d'apprentissage avait été identifié préalablement pour les individus impliqués dans les agressions sexuelles survenues dans un contexte hors ligne (Davies et al., 1997; Park et al., 2008) et suggère qu'en étant en contact avec le système de justice, les individus ont un aperçu de la manière dont une enquête criminelle est conduite et peuvent identifier les erreurs qui les ont conduits à avoir été identifiés la première fois.

[2] Défini comme un « Ensemble de valeurs, de normes et de comportements propres à un groupe social donné et manifestant un écart par rapport à la culture dominante. » Larousse.

Objectif de l'étude

La revue de la littérature nous a permis de constater que les connaissances relatives à l'expertise criminelle des individus impliqués dans des crimes sexuels en ligne étaient limitées. Premièrement, les études font état d'une transposition de l'approche de l'expertise criminelle à la criminalité commise en ligne. Deuxièmement, il a été démontré que plusieurs voies d'acquisition de ces compétences existaient concernant les questions de sécurité par les utilisateurs de contenus virtuels pédophiles. Bien qu'importante dans les perspectives qu'elles ont ouvertes, les connaissances établies par ces études demeurent limitées. L'étude de la sous-culture pédophile se fonde sur une approche globale dans laquelle les questions entourant la gestion de menaces externes ne sont pas approfondies. D'autre part, l'approche méthodologique qualitative a permis l'exploration et l'identification de phénomènes sociaux importants (c.-à-d. la sous-culture pédophile et l'enculturation), mais ne permet pas un approfondissement de sa compréhension. Finalement, d'autres études (p. ex. Chopin, Paquette et Fortin, 2022; Paquette et Fortin, 2021; Seto et al., 2010) ont porté sur des échantillons limités d'individus identifiés et arrêtés par la police, restreignant de fait la validité des résultats proposés. Cette étude propose ainsi d'étendre les connaissances existantes en étudiant la structure latente de la sous-culture pédophile relative aux aspects de cybersécurité. L'objectif est de mieux comprendre quels sont les sujets d'intérêts en matière de cybersécurité pour les utilisateurs de sites pédophiles, comment se structurent ces intérêts et comment s'opère l'enculturation. Ces connaissances nouvelles permettront de renforcer la compréhension des comportements et processus décisionnels d'une population d'individus particulièrement difficile à atteindre et de renseigner les forces de l'ordre sur la manière de fonctionner des utilisateurs de ces forums illégaux. Spécifiquement, cette étude propose de répondre à trois questions de recherche :

QR1 : Est-ce que les thématiques de sécurité discutées sur les forums pédophiles sont structurées de manière homogène ou hétérogène ?

QR2 : Est-ce que les structures de discussion de cybersécurité sont influencées par l'expertise des utilisateurs ?

QR3 : Est-ce que l'intérêt de la communauté pédophile est influencé par des combinaisons particulières de thématiques en cybersécurité ?

Méthode

Données et échantillon

Cette étude a pour objectif de mieux comprendre le comportement des individus impliqués dans la criminalité sur Internet et en particulier sur leur capacité à se prémunir contre les menaces extérieures. Afin de mieux comprendre le comportement des utilisateurs de forums pédophiles, des données ont été collectées puis analysées à partir de trois forums pédophiles identifiés sur le dark web (c.-à-d. la partie du web à laquelle on ne peut accéder que par des navigateurs spécialisés spécialisés, comme le protocole TOR, voir Aldridge et Décary-Hétu, 2016). Particulièrement, les fils de

© Julien Chopin, David Décary-Hétu, Emmanuelle Marois, Léanne Vincendon, 2023

conversations spécialisés sur les questions de sécurités informatiques et de rapport avec les systèmes judiciaires ont été identifiés, extraits sous forme de texte, codés et analysés. Pour identifier les forums pédophiles discutant des questions de cybersécurité, des répertoires de sites sexuels hébergés sur le dark web ont été identifiées à travers des engins de recherche sur le darkweb web. Ces répertoires contenaient des liens vers des forums hébergeant des discussions de pédophiles. La sélection des forums s'est ensuite faite sur la base de deux critères principaux : 1) des sections entières des forums dédiées aux questions de cybersécurité, 2) des conversations suffisamment détaillées sur les questions de cybersécurité, et 3) des thématiques et technologies restreintes aux ères du dark web (2008-2014) et des téléphones cellulaires (2014-présent) (voir Steel et al., 2020). Ce travail d'identification a permis de sélectionner trois forums[3]. Ces trois forums présentent un total de 290 fils de discussion (FDDs) relatifs aux questions de cybersécurités représentant un total de 10 134 messages écrits par 2 715 utilisateurs différents. Chaque FDDs présente en moyenne 35 messages écrits par un nombre moyen de 9 utilisateurs différents. À la date de l'extraction (c.-à-d. le 3 juillet 2022), les messages analysés avaient été vus 4 870 943 fois soit une moyenne de 16 796 fois par FDDs. Finalement, la durée moyenne d'activité (c.-à-d. la différence entre la date du dernier message écrit et la date du premier message) des FDDs est de 518 jours (c.-à-d. environ un an, cinq mois et 2 jours) tandis que leur durée moyenne d'existence (c.-à-d. la différence entre la date d'extraction et la date du premier message) est de 3 071 jours (c.-à-d. environ huit ans, quatre mois et 30 jours). Deux assistantes de recherche qui ont été spécifiquement formées à cet effet ont lu l'ensemble des messages et les ont codés dans une base de données sur la base d'une grille préalablement établie en fonction de la littérature existante sur le sujet. Afin de mesurer le taux d'accord interjuge 10 % des FDDs représentant environ 10 % des messages ont été sélectionnés. Le taux global d'accord est considéré comme excellent puisqu'il atteint 97 % (κ = 0,919). Il est important de noter ici que les données ont été collectées automatiquement à l'aide de logiciels spécialisés de collecte de données en ligne. Aucune image n'a été téléchargée dans le processus de sélection ou de récupération des données, et les messages téléchargés ne contenaient que des discussions sur la cybersécurité.

Mesures

Plusieurs variables qui sont décrites dans le tableau 1 ont été utilisées dans cette étude. Afin de répondre aux objectifs, cette étude s'articule autour de la construction d'un modèle d'analyse de classes latentes qui est décrit dans la section analytique ci-dessous. Plus précisément, cette approche est basée sur la construction d'un modèle principal et d'une analyse de sa validité externe.

Modèle principal. Afin d'explorer l'hétérogénéité du contenu des différents FDDs, un total de sept variables relatives aux thématiques de sécurité ont été utilisées. Ces variables sont toutes dichotomiques (c.-à-d. 0 = absence de la thématique, 1 = présence de la thématique) : 1) stratégies pour se protéger contre les menaces informatiques extérieures (c.-à-d. prévention et/ou identification des logiciels malveillants), 2) stratégies pour éviter la localisation (p. ex. proxy, cryptage du trafic, service d'anonymisation), 3) stratégies pour empêcher l'identification (p. ex. utilisation de services prépayés, cryptomonnaies, utilisation de fausses identités), 4) stratégies visant à éviter l'utilisation de certains services technologiques (p. ex. stockage d'information dans les nuages de données), 5) stratégies visant à faire des recherches en ligne sans laisser de traces (c.-à-d. stratégies en lien avec les moteurs de recherche, témoins de connexion, réseaux sociaux), 6) stratégies visant à obstruer le travail de la justice (p. ex. cryptage du disque dur, destruction d'urgence des données), 7) identifications des facteurs de risques et compréhension des enjeux légaux (c.-à-d. comportements et pratiques à risques pour l'identification par les forces de l'ordre ; risques encourus d'un point de vue légal.

Co-variables de validité externes. Un ensemble de 11 variables additionnelles a été utilisé afin d'améliorer la compréhension du modèle principale et de tester sa validité externe. Dans un premier temps, trois variables dichotomiques ont été utilisées pour mesurer le niveau d'expertise présent dans chaque FDDs : 8) novice (c.-à-d. questions basiques), 9) medium (c.-à-d. poser des questions et chercher du soutien, connaissances de base légèrement avancées), 10) expert (c.-à-d. comprend le fonctionnement des technologies d'anonymat/sécurité et peut l'expliquer, partager ses connaissances avec d'autres membres d'un niveau inférieur au sien). Il est important de noter que dans un FDDs, plusieurs niveaux de compétences peuvent être observés. Dans un deuxième temps, trois variables continues ont été utilisées pour tester l'intérêt de la communauté pédophile en fonction des différentes thématiques traitées. Plus précisément, trois mesures lambda (λ) ont été créées en divisant le nombre de messages, le nombre d'utilisateurs et le nombre de vues par la durée d'activité ou d'existence des fils. Cette décision a été prise afin d'éviter les biais liés à la temporalité qui pourrait faire augmenter les valeurs absolues de ces indicateurs. Les trois variables en question sont donc : 11) λ des messages ($\bar{X}$=1,74, é-t =3,09), 12) λ des utilisateurs ($\bar{X}$=0,92, é-t =1,45), 13) λ du nombre de vues ($\bar{X}$=5,98, é-t =10,91). Troisièmement, nous avons utilisé trois variables dichotomiques pour mesurer le niveau d'expertise du sujet initialement développé dans les FDDs : 14) novice (c.-à-d. questions basiques), 15) medium (c.-à-d. poser des questions et chercher du soutien, connaissances de base légèrement avancées), 16) expert (c.-à-d. questions approfondies concernant entourant le fonctionnement de techniques approfondies). Ces trois variables sont mutuellement exclusives dans le sens ou un FDDs ne peut être qualifié que par une seule d'entre elles. Finalement, deux variables continues de temps ont été utilisées : 17) la durée d'activité (c-.à-d. la différence entre la date du dernier message écrit et la date du premier message), la durée d'existence (c-.à-d. la différence entre la date d'extraction et la date du premier message).

Stratégie analytique

La stratégie analytique utilisée dans cette étude suit un processus en deux étapes. Dans un premier temps, une analyse en classes latentes a été réalisée avec le logiciel Latent Gold V6.0 afin de déterminer s'il existait une organisation latente des sujets de cybersécurité dans les FDDs des trois forums pédophiles qui ont été analysés. L'analyse en classes latentes est une procédure statistique utilisée pour identifier de l'hétérogénéité qui n'est pas directement observable ou mesurable afin de mettre en évidence des schémas d'information sous-jacents dans des données portant

[3] Le nom des forums n'est pas fourni pour des raisons d'éthique et de confidentialité. Ils sont mentionnés dans l'article sous la dénomination de Forum 1, Forum 2 et Forum 3. Néanmoins, ces noms peuvent être fournis sur demande écrite d'autres chercheurs au premier auteur de cette étude.

© Julien Chopin, David Décary-Hétu, Emmanuelle Marois, Léanne Vincendon, 2023

sur une thématique d'apparence homogène (p. ex. les stratégies de cybersécurité) (Collins et Lanza, 2010). Le but de cette procédure consiste à identifier des classes mutuellement exclusives (p. ex. chaque FDDs est distribué dans une seule classe) en utilisant des variables dichotomiques. Concrètement, cette procédure présente l'avantage de se baser sur des techniques de modélisation plus robustes que d'autres techniques de classification (p. ex. classification hiérarchique, partitionnement en k-moyennes) en attribuant à chaque unité statistique une probabilité d'appartenance. Les unités statistiques sont identifiées sur la base de leurs sous-groupes latents et affectés à leurs classes respectives par une méthode de maximum de vraisemblance, qui détermine les taux de probabilité postérieure de chaque cas (Collins et Lanza, 2010). Dans cette étude, sept modèles ont été calculés à partir d'un modèle allant d'une à sept classes (voir Tableau 2). Le critère d'information bayésien (BIC), le BIC ajusté, l'entropie ainsi que le test du rapport de vraisemblance ajusté de Vuong-Lo-Mendell-Rubin ont été utilisés pour évaluer l'ajustement du modèle et déterminer le nombre de classes le plus pertinent à retenir pour le modèle final.

Deuxièmement, nous avons étudié la validité externe des classes du modèle principal identifiées par l'analyse en classes latentes. Cette étape a consisté à examiner les relations distinctes entre les classes identifiées et d'autres indicateurs n'ayant pas servi à construire le modèle principal (p. ex. le niveau de compétence). Cette étape est importante pour vérifier que le modèle principal ne se résume pas à une classification basée seulement sur les indicateurs sur lesquels il a été construit, mais que ces effets s'étendent à des variables périphériques au phénomène étudié. Concrètement, cette procédure a permis de distinguer si les différences identifiées dans le modèle de classification principal, qui étaient basées sur un nombre limité d'indicateurs, se reflétaient dans d'autres indicateurs périphériques du phénomène étudié (p. ex. Deslauriers-Varin et Beauregard, 2010; Jørgensen et Jensen, 1990; Myrseth et Notelaers, 2018). Cette analyse se fonde sur des tests de statistiques bivariées (c'est-à-dire chi-carré et test H de Kruskal-Wallis) afin d'identifier les différences significatives entre les différentes classes.

Résultats

Statistiques descriptives

Le tableau 1 propose une description des différentes variables utilisée dans cette recherche. Les résultats indiquent que les sujets les plus discutés dans les FDDs relatifs à la cybersécurité sont dans l'ordre décroissant : les facteurs de risques conduisant à l'identification par la police et les conséquences judiciaires (60 %),

	n	%		
Stratégies pour se protéger contre les menaces informatiques extérieures	**46**	**15,86**		
Prévention des logiciels malveillants	29	10,00		
Identifications des logiciels malveillants	24	8,28		
Stratégies pour éviter la localisation	**138**	**47,59**		
Proxy	130	44,83		
Cryptage du trafic	38	13,10		
Service d'anonymisation	19	6,55		
Stratégies pour empêcher l'identification	**34**	**11,72**		
Services prépayés	11	3,79		
Utilisation de cryptomonnaies	8	2,76		
Utilisation de fausses identités	7	2,41		
Utilisation de réseau WIFI public	7	2,41		
Utilisation de faux documents	3	1,03		
Stratégies visant à éviter l'utilisation de certains services technologiques	**60**	**20,69**		
Stratégies visant à faire des recherches en ligne sans laisser de trace	**39**	**13,45**		
relatif aux moteurs de recherche	27	9,31		
relatif aux témoins de connexions	16	5,52		
relatif aux réseaux sociaux	7	2,41		
relatif à flash Player	5	1,72		
relatif aux fureteurs	1	0,34		
Stratégies visant à obstruer le travail de la justice	**144**	**49,66**		
Cryptage du disque dur	78	26,90		
Cryptage des communications	64	22,07		
Systèmes d'exploitation anonymes	30	10,34		
Destruction régulière des données/métadonnées	26	8,97		
Destruction d'urgences des données	1	0,34		
Identifications des facteurs de risques et compréhension des enjeux légaux	**173**	**59,66**		
Niveau de compétence des utilisateurs alimentant le fil de conversation				
Novice	214	73,79		
Moyen	227	78,28		
Expert	96	33,10	Asymétrie	Kurtosis
Intérêt de la communauté des utilisateurs de forums pédophiles				
λ du nombre de messages	1,74	3,08	3,09	12,99
λ du nombre de vues	5,98	10,91	6,18	47,13
λ du nombre d'utilisateurs différents	0,92	1,45	A,12	4,88
Niveau de compétence du sujet du fil de conversation				
Novice	142	48,97		
Moyen	102	35,17		
Expert	46	15,86		
Durée de vie	517,66	869,61	2,05	3,61
Durée d'existence	3071,31	1083,14	-0,80	-0,15

Tableau 1 : Statistiques descriptives du contenu des fils de discussion (N=290)

© Julien Chopin, David Décary-Hétu, Emmanuelle Marois, Léanne Vincendon, 2023

les stratégies visant à obstruer le travail de la justice (50 %), les stratégies pour éviter la localisation (48 %), les stratégies visant à éviter l'utilisation de certains services technologiques (21 %), les stratégies pour éviter les menaces informatiques extérieures (16 %) et finalement les stratégies visant à éviter l'identification (12 %).

Analyse en classes latentes

Le tableau 2 décrit les indicateurs de qualité des modèles d'analyse qui ont été calculés. Les indicateurs montrent que la meilleure solution, basés sur le BIC (1961,59) et le BIC ajusté (1810,12) était la solution en quatre classes. Jusqu'à la quatrième classe, le BIC et le BIC ajusté diminuaient tandis qu'à partir de la cinquième classe ils ont tous les deux commencé à augmenter. Ces résultats suggèrent que le compromis entre adéquation et parcimonie a été atteint tandis que la valeur du BIC était la plus faible (Schwartz, 1978). L'entropie pour la solution à 4 classes est élevée (0,88), ce qui signifie que les prédicteurs utilisés étaient appropriés pour classer les unités statistiques et que les classes présentaient des différences importantes entre elles (Schwartz, 1978). Le test du rapport de vraisemblance ajusté de Vuong-Lo-Mendell-Rubin a suggéré que le modèle à quatre classes améliorait significativement l'ajustement du modèle à trois classes (p <.001) alors que ça n'était pas le cas du modèle en cinq classes (p =.097).

Le tableau 3 et la Figure 1 présentent les résultats du modèle en quatre classes qui a été retenu. La classe incluant le plus de FDDs est la classe 1 (36 % des FDDs ; n=104) tandis que la classe la moins prévalente est la classe 4 (17 % des FDDs ; n=50).

La classe 1 (Stratégies réactives de confrontation avec la justice) représente la classe la plus prévalente de toutes. Les FDDs qui sont inclus dans cette classe ont une probabilité très élevée de porter sur des sujets relatifs aux stratégies visant à obstruer le travail de la justice (1,00)[4] ainsi que sur les facteurs de risques d'identification par la police et la compréhension des enjeux légaux y étant associés (1,00).

La classe 2 (Stratégies proactives basiques) inclut 25 % (n=72) des FDDs analysés et est la deuxième plus prévalente. Les FDDs inclus dans cette classe ont une plus forte probabilité de porter sur les stratégies pour éviter la localisation (0,74) et une probabilité moyenne (0,50), mais néanmoins supérieure à celle de toutes les autres classes de porter sur les stratégies visant à faire des recherches en ligne sans laisser de traces.

[4] Les chiffres entre parenthèse représentent les probabilités d'appartenance moyenne

	LL	BIC	AIC	BIC ajusté	L^2	ddl	VLMR	Valeur p	Entropie (R^2)
1 classe	-1091,24	2222,17	2196,48	2199,97	2182,48	283,00	-	-	1,00
2 classes	-920,33	1959,73	1882,66	1893,13	1840,66	269,00	341,82	0,000	0,93
3 classes	-881,57	1965,51	1833,15	1850,60	1763,15	255,00	77,51	0,000	0,89
4 classes	**-843,84**	**1961,59**	**1785,69**	**1810,12**	**1687,69**	**241,00**	**75,46**	**0,000**	**0,88**
5 classes	-827,82	2012,85	1781,64	1813,06	1655,64	227,00	32,04	0,097	0,84
6 classes	-811,64	2059,87	1777,29	1815,69	1623,29	213,00	32,36	0,000	0,84
7 classes	-804,35	2124,67	1790,71	1836,09	1608,71	199,00	14,58	0,464	0,84

Les caractères en gras indiquent le modèle sélectionné.
BIC : critère d'information bayésien.
AIC : critère d'information d'Akaike.
VLMR : Test du rapport de vraisemblance Vuong-Lo-Mendell-Rubin.

Tableau 2 : Indicateurs de qualité des modèles d'analyse en classes latentes (N=290)

		Classe 1 Stratégies réactives de confrontation avec la justice	Classe 2 Stratégies proactives basiques	Classe 3 Stratégies de lutte contre les menaces non judiciaires	Classe 4 Stratégies proactives avancées
	%	35,86 %	24,83 %	22,07 %	17,24 %
	n	104	72	64	50
1. Stratégies pour se protéger contre les menaces informatiques extérieures		0,00	0,03	0,67	0,02
2. Stratégies pour éviter la localisation		0,38	0,74	0,09	0,94
3. Stratégies pour empêcher l'identification		0,05	0,03	0,03	0,70
4. Stratégies visant à éviter l'utilisation de certains services technologiques		0,14	0,17	0,00	0,66
5. Stratégies visant à faire des recherches en ligne sans laisser de traces		0,02	0,50	0,00	0,02
6. Stratégies visant à obstruer le travail de la justice		1,00	0,00	0,00	0,80
7. Identifications des facteurs de risques et compréhension des enjeux légaux		1,00	0,17	0,16	0,94

Tableau 3 : Modèle de classification en quatre classes latentes du contenu des fils de discussion en fonction des probabilités d'appartenance (N=290)

© Julien Chopin, David Décary-Hétu, Emmanuelle Marois, Léanne Vincendon, 2023

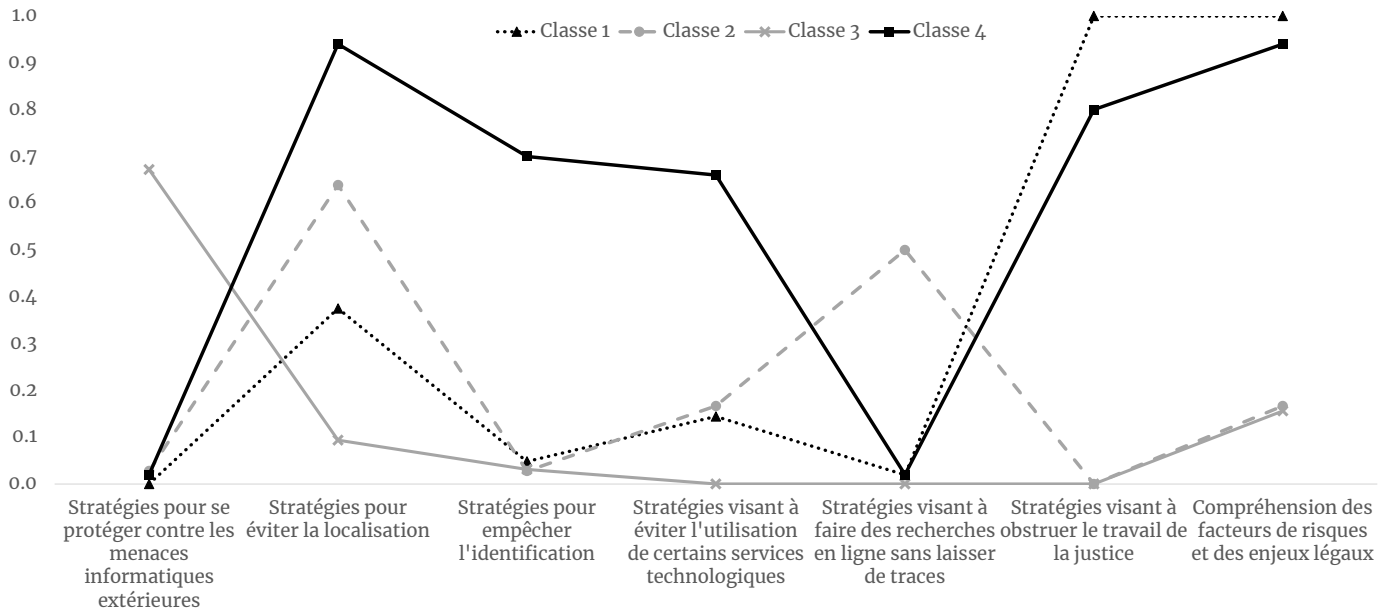

Figure 1 : Profil des quatre classes latentes en fonction du contenu des fils de discussion - Probabilités moyennes (N=290)

La classe 3 (Stratégies de lutte contre les menaces non judiciaires) est la troisième plus prévalente et inclut 22 % (n=64) des FDDs. Cette classe est caractérisée par la présence de FDDs centrés uniquement sur les stratégies visant à se protéger contre les menaces informatiques extérieures (0,67).

La classe 4 (Stratégies proactives avancées) est la classe incluant le moins de FDDs avec 17 % d'entre eux (n=50). Cette classe inclut des FDDs ayant une forte probabilité de traiter des stratégies pour éviter la localisation (0,94), des stratégies pour empêcher l'identification (0,70), pour obstruer le travail de la justice (0,80) et pour identifier les facteurs de risques d'identification par la police ainsi que la compréhension des enjeux légaux (0,94).

Analyse de validité externe

Afin d'évaluer la validité externe du modèle principal en quatre classes, des analyses bivariées ont été effectuées sur 11 variables additionnelles et les résultats sont présentés dans le tableau 4. Sur les 11 variables testées, 9 présentent des différences significatives entre les classes. Les résultats indiquent que les utilisateurs présentaient plus souvent un niveau de compétence médium dans les FDDs inclus dans les classes 2 et 4 que dans les classes 1 et 3 (χ^2 = 130,28, p < .001, φ_c = 0,67) tandis que les utilisateurs présentant un niveau de compétence expert sont plus souvent inclus dans les classes 1 et 4 que dans les classes 2 et 3 (χ^2 = 29,99, p < .001, φ_c = 0,32). Concernant l'intérêt de la communauté par rapport au contenu des FDDs, la classe 2 présente l'λ du nombre de messages (H de Kruskall-Wallis = 9,09, ddl = 3, p = ,028, η^2 = 0,02) ainsi que l'λ du nombre d'utilisateurs différents le plus élevé (H de Kruskall-Wallis = 21,23, ddl = 3, p < ,001, η^2 = 0,04). Les FDDs inclus dans la classe 4 présentaient l'λ du nombre de vues moyen le plus élevé (H de Kruskall-Wallis = 60,93, ddl = 3, p < ,001, η^2 = 0,17). Les sujets traités dans les FDDs de la classe 3 étaient plus souvent d'un niveau novice (χ^2 = 30,45, p < .001, φ_c = 0,32), tandis que ceux des classes 2 et 4 étaient plus souvent de niveau moyen (χ^2 = 15,26, p < .001, φ_c = 0,27). Finalement, les sujets traités dans les FDDs inclus dans la classe 4 étaient plus souvent de niveau expert (χ^2 = 15,26, p < .001, φ_c = 0,23). Les FDDs inclus dans la classe 4 présentaient la durée d'existence moyenne la plus longue (H de Kruskall-Wallis = 34,54, ddl = 3, p < ,001, η^2 = 0,13).

Discussion

L'objectif de cette étude consistait à développer le corpus de connaissances existantes concernant l'acquisition de compétences en matière de cybersécurité des individus impliqués dans des crimes sexuels commis dans un contexte virtuel. Spécifiquement le but était d'identifier les structures latentes qui pouvaient exister dans FDDs par rapport aux différentes thématiques discutées par les utilisateurs de forums pédophiles et de tester différents corrélats relatifs à l'expertise et à l'intérêt de la communauté. Cette étude a été encadrée par l'approche du choix rationnelle (Cornish et Clarke, 1986; Cornish et Clarke, 1987) et particulièrement un de ses approfondissements : l'expertise criminelle (Reale, 2022). Dans le but d'étudier une population particulièrement difficile à atteindre, les consommateurs de matériel d'exploitation sexuelle d'enfants en ligne, nous avons analysé le contenu virtuel qu'ils ont consommé en matière de cybersécurité afin de mieux comprendre leurs décisions et comportements (Holt et al., 2010; Westlake et Bouchard, 2016). L'analyse réalisée se base ainsi sur des données collectées dans trois forums pédophiles identifiés sur le dark web et particulièrement actifs sur les questions de cybersécurités. Les FDDs relatifs à ce sujet ont été codés puis analysés par le biais d'une procédure d'analyse en classes latentes.

Sous-culture pédophile et enculturation à dimensions variables en matière de sécurité

Les résultats de nos analyses laissent percevoir plusieurs points d'interprétation intéressants. Premièrement, l'analyse des statistiques descriptives permet de tirer plusieurs enseignements. En ce qui concerne le niveau d'expertise, que ce soit celui des sujets développés dans les FDDs ou que ce soit celui des utilisateurs participants à ces FDDs, nous observons une structure pyramidale confirmant l'idée que les individus doués des compétences supérieures représentent la minorité de la population, que ce soit

© Julien Chopin, David Décary-Hétu, Emmanuelle Marois, Léanne Vincendon, 2023

	Classe 1. Stratégies réactives de confrontation avec la justice		Classe 2. Stratégies proactives basiques		Classe 3. Stratégies de lutte contre les menaces non judiciaires		Classe 4. Stratégies proactives avancées		χ^2/H de Kruskal Wallis	φ_c/η^2
	n	%	n	%	n	%	n	%		
Niveau de compétence des utilisateurs alimentant le fil de conversation										
Novice	77_a	74,04 %	56_a	77,78 %	47_a	73,44 %	34_a	68,00 %	1,46	0,07
Moyen	87_a	83,65 %	72_b	100,00 %	18_c	28,13 %	50_b	100,00 %	130,28***	0,67
Expert	49_a	47,12 %	21_b	29,17 %	5_c	7,81 %	$21_{a,b}$	42,00 %	29,99***	0,32
Intérêt de la communauté des utilisateurs de forums pédophiles										
λ du nombre de messages (moyenne)	1,36		1,90		2,32		1,54		9.09*[1]	0,02[2]
λ du nombre de vues (moyenne)	4,19		2,39		5,50		15,49		60.93***[1]	0,17[2]
λ du nombre d'utilisateurs différents (moyenne)	0,71		1,17		1,25		0,57		21.23***[1]	0,04[2]
Niveau de compétence du sujet initial du fil de conversation										
Novice	56_a	53,85 %	31_a	43,06 %	45_b	70,31 %	10_c	20,00 %	30,45***	0,32
Moyen	27_a	25,96 %	34_b	47,22 %	14_a	21,88 %	27_b	54,00 %	21,19***	0,27
Expert	$21_{a,b}$	20,19 %	$7_{b,c}$	9,72 %	3_c	4,69 %	14_a	28,00 %	15,26***	0,23
Durée de vie en jours (moyenne)	447,94		295,15		356,55		1189,3		34.54***[1]	0,13[2]
Durée d'existence en jours (moyenne)	3067,38		3117,26		2903,23		3228,44		210[1]	0,01[2]

Notes. *p < ,05. ***p < ,001.
Comparaisons par paires : chaque lettre en indice dénote un sous-ensemble du modèle à 4 classes dont les proportions des colonnes ne diffèrent pas significativement les unes des autres au niveau de 0,05.
[1] : H de Kruskal Wallis
[2] : Êta carré

Tableau 4 : Analyse de la validité externe du modèle en quatre classes en fonction du contenu des fils de discussion (N=290)

dans un contexte criminel ou non (Ericsson et al., 2018; Paquette et Fortin, 2021; Reale et al., 2021b). D'autre part, la prévalence des sujets traités dans les FDDs qui ont été utilisés suggère que la communauté pédophile s'est prioritairement intéressée à des sujets présentant un niveau d'abstraction plus élevé (c.-à-d. la compréhension et à l'identification des facteurs de risques d'être identifiés par la police), puis par des stratégies réactives (c.-à-d. visant à obstruer le travail de la justice), et finalement aux stratégies proactives (p. ex. empêcher la localisation, l'identification, etc.). Ce résultat renforce l'idée d'une majorité d'individus avec des compétences limitées tandis qu'une minorité vise le développement de compétences plus spécifiques et efficaces (c.-à-d. les stratégies proactives) pour anticiper les risques. Deuxièmement, les analyses de classes latentes révèlent l'existence d'une structure hétérogène dans la distribution des différentes thématiques de cybersécurité sur les forums que nous avons analysés. Ce résultat vient ajouter aux connaissances produites par Holt et al. (2010) en identifiant des sous-thèmes de sujets relatifs à la sécurité. Les FDDs les plus nombreux sont centrés sur les stratégies réactives de confrontation avec la justice (classe 1), puis sur les stratégies proactives basiques (classe 2), ensuite sur stratégies de lutte contre les menaces non judiciaires (classe 3), et finalement sur les stratégies proactives avancées (classe 4). Ce résultat renforce l'idée que le niveau d'abstraction vs spécialité ainsi que l'effet proactif vs réactif des stratégies pourraient être considérés comme des indicateurs importants de l'expertise criminelle dans un contexte virtuel. Troisièmement, l'analyse des corrélats du modèle principale indique deux résultats importants. S'il est important de s'intéresser aux utilisateurs de ces FDDs, c'est-à-dire ceux qui y contribuent activement, il est également pertinent de porter le regard vers ceux qui y ont une participation passive en visionnant le contenu et en se nourrissant des informations qui y sont disséminées. Le nombre de vues de chaque FDDs est une information précieuse puisqu'elle renseigne sur le comportement de la majorité silencieuse d'utilisateurs de ces forums. Les résultats suggèrent ainsi que les FDDs les moins nombreux (classe 4), mais présentant le niveau d'expertise le plus élevé sont également ceux présentant le plus grand λ du nombre de vues. Ce résultat vient confirmer l'idée d'un processus d'enculturation en matière de sécurité dans lequel la majorité d'individus novices viennent s'informer et acquérir des compétences par le biais de ceux ayant des compétences d'expertises supérieures (Holt et al., 2010). L'autre point important est la durée de vie des FDDs qui est positivement corrélée à la classe 4 incluant les FDDs discutant les stratégies proactives avancées. La durée de vie d'un contenu virtuel est un indicateur important de sa pertinence et de sa qualité (see Gonzalez et Palacios, 2004; Hernández et al., 2009; Rekik et al., 2018). Dans le contexte de cette étude, nous observons ainsi que les FDDs présentant le contenu le plus expert sont ceux ayant la durée de vie la plus longue. Il se pourrait que certains FDDs soient le vecteur privilégié de certains utilisateurs experts qui contribuent à les faire vivre de manière régulière. D'autre part, les résultats suggèrent que l'intérêt de la communauté pédophile est influencé par les combinaisons de thématiques constituant les différentes classes. En effet, les indicateurs permettant de mesurer l'intérêt (i.e., λ du nombre de vues, λ du nombre d'utilisateurs) varient significativement entre les classes. Ainsi, nous observons que le λ du nombre de vues est beaucoup plus important pour la classe 4

© Julien Chopin, David Décary-Hétu, Emmanuelle Marois, Léanne Vincendon, 2023

tandis que le λ du nombre d'utilisateurs est plus important pour la combinaison de thématiques contenues dans la classe 3.

Une nouvelle classification de la sous-culture pédophile en matière de sécurité

L'analyse en classes latentes a montré qu'il existait quatre classes distinctes de thématiques traitées par les FDDs extraits des forums pédophiles.

Stratégies réactives de confrontation avec la justice. Ce premier groupe de FDDs s'appuie particulièrement sur les facteurs de risque d'identification par la police et les stratégies réactives. Il est intéressant de voir que cette classe recense la plus grande prévalence de FDDs. Il se pourrait qu'ils concernent les utilisateurs ayant des démêlés avec la justice et qui cherchent de l'aide de la part de la communauté (Jenkins, 2001; Quayle et Taylor, 2002). On observe par ailleurs que le niveau d'expertise des utilisateurs est globalement élevé par rapport aux autres classes. Ceci pourrait être associé aux discussions relatives aux stratégies réactives spécifiques pouvant permettre de limiter les conséquences judiciaires (p. ex. cryptage du disque dur, cryptage des communications, destruction d'urgence des données).

Stratégies proactives basiques. Les FDDs inclus dans cette classe sont relatives aux stratégies proactives visant à éviter la localisation et dans une moindre mesure à éviter de laisser des traces lors de recherche en ligne. Cette classe est la deuxième plus prévalente en nombre de FDDs mais intéresse peu la communauté en regard des différents indicateurs qui ont été utilisés (c.-à-d. différents λ). D'autre part, les FDDs inclus dans cette catégorie présentent la durée moyenne d'existence la plus faible avec un niveau d'expertise limité. Comme cela est discuté par les recherches dans le domaine du e-commerce et appliqué en criminologie : plus le contenu virtuel a une durée de vie limitée, moins il est d'intérêt pour la communauté qu'il cible (see Gonzalez et Palacios, 2004; Hernández et al., 2009; Rekik et al., 2018; Westlake et Bouchard, 2016). Si les sujets développés pouvaient être d'importance, le faible niveau d'expertise des utilisateurs et des sujets traités vient probablement détourner l'intérêt des autres membres de la communauté.

Stratégies de lutte contre les menaces non judiciarisées. Les FDDs inclus dans cette classe sont intéressants dans la mesure où ils concernent des stratégies visant des actions de sécurité contre des menaces extérieures non judiciaires telles que les logiciels malveillants ou encore les virus. Il est intéressant de constater ce que cette catégorie de FDDs est celle qui présente les λ du nombre d'utilisateurs différents et de messages les plus importants. Ce résultat est somme toute assez logique puisque ces compétences sont plus communes et se posent à chaque utilisateur de matériel informatique (Idika et Mathur, 2007). Ce sujet ne nécessite pas un niveau de compétence particulier et d'ailleurs les utilisateurs experts sont les moins prévalents, tandis que les sujets traités nécessitent un niveau de compétence basique.

Stratégies proactives avancées. Cette classe qui est la moins prévalente en nombre de FDDs est en même temps la plus intéressante. Elle inclut dans un nombre très restreint de FDDs caractérisés par les sujets et utilisateurs les plus experts. Ces FDDs traitent de tous les sujets du continuum sécuritaire : identification des facteurs de risques, stratégies proactives, puis stratégies réactives. Bien que peu nombreux, les FDDs inclus dans cette classe pourraient être ceux les plus importants dans le processus d'enculturation créant un véritable canal de discussion et de transmission entres les membres de la communauté pédophile (Holt et al., 2010; Jenkins, 2001). Un système hiérarchique très clair s'observe entre les utilisateurs passifs (c.-à-d. λ du nombre de vues) et les utilisateurs novices d'une part, questionnent et s'informent auprès des utilisateurs de niveau moyen dans une moindre mesure et des utilisateurs de niveau expert.

Conclusion

Cette étude s'est intéressée à la sous-culture pédophile en ligne en matière de cybersécurité. En utilisant une méthode visant à mieux comprendre les décisions et comportements des utilisateurs en ligne en analysant le contenu virtuel avec lequel ils interagissent, il a été possible d'approfondir des connaissances sur une population réputée difficile à atteindre et étudier. Les résultats ont indiqué que la sous-culture pédophile en matière cybersécurité constituait un ensemble hétérogène se structurant en quatre sous-ensembles. Ces sous-ensembles constitués sur la base de combinaison de thématiques de sécurité se sont avérés particulièrement sensibles aux indicateurs externes d'expertise et d'intérêt de la communauté. L'analyse de ces différentes classes a permis de dresser une hiérarchie des thématiques, de leur niveau d'expertise et de l'intérêt qu'elles présentaient. Ces résultats permettent de renforcer l'hypothèse d'existence d'une sous-culture pédophile sur les thématiques de sécurité se basant sur un processus d'enculturation des membres les plus experts envers les autres.

Bien que novatrice, cette étude n'est pas sans limitations. Premièrement, bien que nous ayons amélioré la portée des résultats comparativement aux études basées sur des échantillons de police (c.-à-d. inclusions d'individus non judiciarisés), cette étude se base sur l'analyse de FDDs totalement dévolu à ce sujet sur des forums pédophiles. Il est tout à fait possible que les utilisateurs de ces FDDs en particulier présentent une sensibilité particulière aux sujets de sécurité. D'autre part, les FDDs analysés proviennent de forums identifiés sur le dark web impliquant un certain niveau de connaissances de la communauté pour s'y rendre. Ces deux aspects contribuent à créer un biais de sélection dans notre échantillon entraînant certainement une surestimation des compétences en matière de sécurité des membres de la communauté pédophile en ligne. Deuxièmement, une des mesures importantes de l'importance des sujets de sécurité pour la communauté pédophile repose sur le nombre de vues relatif à chaque FDD. Il n'a malheureusement pas été possible d'établir que chaque vue corresponde à un individu unique. Il est ainsi tout à fait possible qu'un individu réalise plusieurs vues des différents FDDs. Dans le même ordre d'idée, nous ne pouvons exclure qu'une personne possède plusieurs comptes utilisateurs.

Cette étude présente plusieurs implications. D'un point de vue théorique, les résultats permettent de confirmer une fois encore la transposabilité du cadre de l'expertise criminelle à la criminalité commise dans un contexte virtuel. Les résultats montrent clairement un système pyramidal des niveaux de compétences suggérant qu'une minorité d'individus présentent un degré d'expertise élevé. Nos résultats confirment également l'existence d'une sous-culture pédophile sur les sujets de sécurité, structurée de façon hétérogène. Cette structure des thématiques est influencée

© Julien Chopin, David Décary-Hétu, Emmanuelle Marois, Léanne Vincendon, 2023

par le niveau d'expertise des utilisateurs et impacte l'intérêt de la communauté. La présence de thématiques transversales présentant un niveau d'expertise élevé contribue fortement au développement du processus d'enculturation. Dans une perspective plus pratique, les résultats indiquent qu'un nombre limité d'individus contribue à former une grande partie de la communauté pour éviter les menaces extérieures et particulièrement celles relatives au système judiciaire. Il y a fort à parier que si les efforts étaient concentrés sur l'identification de ces individus experts, le processus d'enculturation serait fortement affecté et rendrait la communauté pédophile plus vulnérable.

Les études futures devraient reproduire cette étude avec d'autres forums afin de tester la validité des résultats proposés. De plus, la méthodologie consistant à utiliser les contenus virtuels pour mieux comprendre les phénomènes criminels devrait être étendue afin d'investiguer les autres composantes de la sous-culture pédophile. Finalement, l'un des points importants réside dans la capacité des recherches futures à atteindre un échantillon plus représentatif de la communauté pédophile en capturant les comportements et caractéristiques de ceux ne naviguant pas nécessairement sur les FDDs relatifs aux aspects sécuritaires. Cela pourrait être fait par le biais d'un sondage auto reporté des pratiques en matière de sécurité qui pourrait être distribuée sur différents forums pédophiles.

Références

Acar, K. V. (2017). Child abuse materials as digital goods: Why we should fear new commercial forms.

Aldridge, J. et Décary-Hétu, D. (2016). Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets. International Journal of Drug Policy, 35, 7-15. https://doi.org/10.1016/j.drugpo.2016.04.020

American Psychiatric Association. (2013). Diagnostic and statistical manual of mental disorders: DSM-5™ (5the éd.). American Psychiatric Publ. http://www.psychiatry.org/psychiatrists/practice/dsm/dsm-5/online-assessment-measures

Beauregard, E. et Bouchard, M. (2010). Cleaning up your act: Forensic awareness as a detection avoidance strategy. Journal of Criminal Justice, 38(6), 1160-1166. https://doi.org/10.1002/car.2308

Brake, M. (1980). The sociology of youth culture and youth subcultures. Routledge & Kegan.

Caneppele, S. et Aebi, M. F. (2019). Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and hybrid crimes. Policing: A Journal of Policy and Practice, 13(1), 66-79. https://doi.org/10.1093/police/pax055

Cherbonneau, M. et Copes, H. (2005). 'Drive it like you Stole it' Auto Theft and the Illusion of Normalcy. British Journal of Criminology, 46(2), 193-211. https://doi.org/10.1093/bjc/azi059

Chohan, U. W. (2017). A history of bitcoin. Disponible à SSRN 3047875.

Chopin, J., Paquette, S. et Beauregard, E. (2022). Is There an Expert Stranger "Rapist" Sexual Abuse, 34(1). https://doi.org/10.1177/1079063221993478

Chopin, J., Paquette, S. et Fortin, F. (2022). Geeks and Newbies: Investigating the Criminal Expertise of Online Sex Offenders. Deviant Behavior, 1-17. https://doi.org/10.1080/01639625.2022.2059417

Collins, L. M. et Lanza, S. T. (2010). Latent class and latent transition analysis: With applications in the social, behavioral, and health sciences. Wiley.

Copes, H. et Cherbonneau, M. (2006). The key to auto theft: emerging methods of auto theft from the offenders' perspective. British Journal of Criminology, 46(5), 917-934. https://doi.org/10.1093/bjc/azl001

Cornish, D. B. et Clarke, R. V. (1986). Introduction. Dans D. B. Cornish et R. V. Clarke (dir.), The Reasoning Criminal: Rational choice perspectives on offending (p. 1-18). Springer-Verlag.

Cornish, D. B. et Clarke, R. V. (1987, 1987). Understanding crime displacement: An application of rational choice theory. Criminology, 25(4), 933-948. https://doi.org/10.1111/j.1745-9125.1987.tb00826.x

Cornish, D. B. et Clarke, R. V. (2008). The rational choice perspective. Dans R. Wortley et L. Mazerolle (dir.), Environmental Criminology and Crime Analysis. Willan Publishing.

Davies, A., Wittebrood, K. et Jackson, J. L. (1997). Predicting the criminal antecedents of a stranger rapist from his offence behaviour. Science & Justice, 37(3), 161-170. https://doi.org/10.1016/S1355-0306(97)72169-5

Deslauriers-Varin, N. et Beauregard, E. (2010, 2010/09//). Victims' routine activities and sex offenders' target selection scripts: A latent class analysis. Sexual Abuse, 22(3), 315-342. https://doi.org/10.1177/1079063210375975

Durkin, K. F. (1997). Misuse of the Internet by pedophiles: Implications for law enforcement and probation practice. Fed. Probation, 61, 14.

Durkin, K. F. et Bryant, C. D. (1999). Propagandizing pederasty: A thematic analysis of the on-line exculpatory accounts of unrepentant pedophiles. Deviant Behavior, 20(2), 103-127. https://doi.org/10.1080/016396299266524

Ericsson, K. A., Hoffman, R. R., Kozbelt, A. et Williams, A. M. (2018). The Cambridge handbook of expertise and expert performance. Cambridge University Press.

Fontana-Rosa, J. C. (2001). Legal competency in a case of pedophilia: Advertising on the Internet. International Journal of Offender Therapy and Comparative Criminology, 45(1), 118-128. https://doi.org/10.1177/0306624X0145100

Fortin, F. (2014). C'est ma collection mais c'est bien plus que ça: analyse des processus de collecte et de l'évolution des images dans les collections de pornographie juvénile [Université de Montréal].

Gonzalez, F. M. et Palacios, T. B. (2004). Quantitative evaluation of commercial web sites:: an empirical study of Spanish firms. International Journal of information management, 24(4), 313-328. https://doi.org/10.1016/j.ijinfomgt.2004.04.009

© Julien Chopin, David Décary-Hétu, Emmanuelle Marois, Léanne Vincendon, 2023

Hernández, B., Jiménez, J. et Martín, M. J. (2009). Key website factors in e-business strategy. International Journal of information management, 29(5), 362-371. https://doi.org/10.1016/j.ijinfomgt.2008.12.006

Holt, T. J., Blevins, K. R. et Burkert, N. (2010). Considering the pedophile subculture online. Sexual Abuse, 22(1), 3-24. https://doi.org/10.1177%2F1079063209344979

Idika, N. et Mathur, A. P. (2007). A survey of malware detection techniques. Purdue University, 48(2), 32-46.

Jenkins, P. (2001). Beyond tolerance: Child pornography on the Internet. University Press.

Jørgensen, P. et Jensen, J. (1990). Latent class analysis of deluded patients. Psychopathology, 23(1), 46-51. https://doi.org/10.1159/000284637

Krone, T., Smith, R. G., Cartwright, J., Hutchings, A., Tomison, A. et Napier, S. (2017). Online child sexual exploitation offenders: A study of Australian law enforcement data. Criminology Research Grants, 77, 1213.

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: overview and issues. Crime, Law and Social Change, 67(1), 3-20. https://doi.org/10.1007/s10611-016-9645-3

Linde, A. et Aebi, M. (2020). La criminologie comparée à l'heure de la société numérique : Les théories traditionnelles peuvent-elles expliquer les tendances de la cyber-délinquance? Revue Internationale de Criminologie et de Police Technique et Scientifique, 4(20), 387-414.

Loeb, J. (2017). Europol study assesses technology for fighting online child abuse [News Briefing]. Engineering & Technology, 12(10), 8-8. https://doi.org/10.1049/et.2017.1011

McCarthy, J. A. (2010). Internet sexual activity: A comparison between contact and non-contact child pornography offenders. Journal of sexual aggression, 16(2), 181-195. https://doi.org/10.1080/13552601003760006

Myrseth, H. et Notelaers, G. (2018). A latent class approach for classifying the problem and disordered gamers in a group of adolescence. Frontiers in psychology, 9, 2273. https://doi.org/10.3389/fpsyg.2018.02273

Nee, C. (2015). Understanding expertise in burglars: From pre-conscious scanning to action and beyond. Aggression and Violent Behavior, 20, 53-61. https://doi.org/10.1016/j.avb.2014.12.006

Nee, C. et Meenaghan, A. (2006). Expert decision making in burglars. British Journal of Criminology, 46(5), 935-949. https://doi.org/10.1093/bjc/azl013

Nee, C. et Taylor, M. (2000). Examining burglars' target selection: Interview, experiment or ethnomethodology? Psychology, Crime & Law, 6(1), 45-59. https://doi.org/10.1080/10683160008410831

Nee, C. et Ward, T. (2015). Review of expertise and its general implications for correctional psychology and criminology. Aggression and Violent Behavior, 20, 1-9. https://doi.org/10.1016/j.avb.2014.12.002

Nee, C., White, M., Woolford, K., Pascu, T., Barker, L. et Wainwright, L. (2015). New methods for examining expertise in burglars in natural and simulated environments: preliminary findings. Psychology, Crime & Law, 21(5), 507-513. https://doi.org/10.1080/1068316X.2014.989849

Owen, G. et Savage, N. (2015). The Tor dark net. https://policycommons.net/artifacts/1223621/the-tor-dark-net/1776697/

Paquette, S. et Fortin, F. (2021). Les traces numériques laissées par les cyberdélinquants sexuels: identités virtuelles et protection de l'anonymat. Revue Internationale de Criminologie et de Police Technique et Scientifique.

Park, J., Schlesinger, L. B., Pinizzotto, A. J. et Davis, E. F. (2008). Serial and single-victim rapists: differences in crime-scene violence, interpersonal involvement, and criminal sophistication. Behavioral Sciences & the Law, 26(2), 227-237. https://doi.org/10.1002/bsl.804

Penna, L., Clark, A. et Mohay, G. (2005). Challenges of automating the detection of paedophile activity on the internet. Dans. First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05).

Quayle, E. et Taylor, M. (2002). Child pornography and the Internet: Perpetuating a cycle of abuse. Deviant Behavior, 23(4), 331-361. https://doi.org/10.1080/01639620290086413

Reale, K. (2022). Criminal Expertise and Sexual Violence: An Examination of the Crime-Commission Process [Simon Fraser University]. https://summit.sfu.ca/item/34855

Reale, K., Beauregard, E. et Chopin, J. (2021a). Criminal Expertise and Sexual Violence: Comparing the Crime-Commission Process Involved in Sexual Burglary and Sexual Robbery Criminal Justice and Behavior. https://doi.org/10.1177/00938548211023541

Reale, K., Beauregard, E. et Chopin, J. (2021b). Expert Versus Novice: Criminal Expertise in Sexual Burglary and Sexual Robbery Sexual Abuse. https://doi.org/10.1177/10790632211024236

Rekik, R., Kallel, I., Casillas, J. et Alimi, A. M. (2018). Assessing web sites quality: A systematic literature review by text and association rules mining. International Journal of information management, 38(1), 201-216. https://doi.org/10.1016/j.ijinfomgt.2017.06.007

Sanger, D. E. et Chen, B. X. (2014). Signaling post-Snowden Era, new iPhone locks out NSA. New York Times, 26.

Seto, M. C., Reeves, L. et Jung, S. (2010). Explanations given by child pornography offenders for their crimes. Journal of sexual aggression, 16(2), 169-180. https://doi.org/10.1080/13552600903572396

Steel, C. M., Newman, E., O'Rourke, S. et Quayle, E. (2020). An integrative review of historical technology and countermeasure usage trends in online child sexual exploitation material offenders. Forensic Science International: Digital Investigation, 33, 300971. https://doi.org/10.1016/j.fsidi.2020.300971

Sutherland, E. H. (1937). The professional thief. Journal of Criminal Law and Criminology (1931-1951), 161-163.

Taylor, M., Quayle, E. et Holland, G. (2001). Child pornography, the Internet and offending. The Canadian Journal of Policy Research, 2(2), 94-100.

© Julien Chopin, David Décary-Hétu, Emmanuelle Marois, Léanne Vincendon, 2023

Topalli, V. (2005). Criminal expertise and offender decision-making: An experimental analysis of how offenders and non-offenders differentially perceive social stimuli. The British Journal of Criminology, 45(3), 269-295. https://doi.org/10.1093/bjc/azh086

Ward, T. (1999). Competency and deficit models in the understanding and treatment of sexual offenders. Journal of sex research, 36(3), 298-305. https://doi.org/10.1080/00224499909552000

Westlake, B. G. et Bouchard, M. (2016). Criminal careers in cyberspace: Examining website failure within child exploitation networks. Justice Quarterly, 33(7), 1154-1181. https://doi.org/10.1080/07418825.2015.1046393

Wolak, J., Finkelhor, D. et Mitchell, K. (2005). Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study.

Wolak, J., Finkelhor, D. et Mitchell, K. (2011). Child pornography possessors: Trends in offender and case characteristics. Sexual Abuse, 23(1), 22-42. https://doi.org/10.1177%2F1079063210372143

Wolak, J., Mitchell, K. et Finkelhor, D. (2003). Internet sex crimes against minors: The reponse of law enforcement. National Center for Missing and Exploited Children.

Young, J. (2010). Subcultural Theories: Virtues and Vices. Dans R. Agnew et J. Kaufman (dir.), Anomie, Strain and Subcultural Theories of Crime (p. 110-135). Ashgate.

© Julien Chopin, David Décary-Hétu, Emmanuelle Marois, Léanne Vincendon, 2023