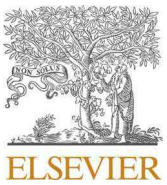
Journal of Criminal Justice 86 (2023) 102060



Contents lists available at ScienceDirect

Journal of Criminal Justice

journal homepage: www.elsevier.com/locate/jcrimjus

Dark web pedophile site users' cybersecurity concerns: A lifespan and survival analysis

Julien Chopin [a,b,c,*], David Décary-Hétu [a]

[a] International Centre for Comparative Criminology, University of Montreal, Montreal, QC H3C 3J7, Canada
[b] Terrorism, Violence and Security Institute Research Centre, Simon Fraser University, Burnaby, BC V5A 1S6, Canada
[c] School of Social Work and Criminology, Laval University, Quebec, QC G1V 0A6, Canada

ARTICLE INFO

Keywords:
Cybersecurity
Dark web pedophile forums
Criminal expertise
Lifespan analysis
Survival analysis

ABSTRACT

Purpose: This paper explores the concept of criminal expertise within the context of online pedophile community and applies rational choice theory to understand the decision-making processes of offenders. Specifically, this study aims to explore the cybersecurity concerns of dark web pedophile forum users known to be a hard-to-reach offender population.

Methods: Sequential generalized linear model and Cox proportional hazard regression model were used to examine cybersecurity themes predicting both the lifespan and survival of 290 cybersecurity-related threads extracted from three pedophile forums identified on the dark web.

Results: Results showed that that risk factors for law enforcement identification-related topics were the most predictive of threads' lifespan and survival. Moreover, topics related to proactive protection strategies were more predictive than those related to reactive ones. Finally, threads with a superior skill level were more likely to survive than other types of content.

Conclusion: This study builds upon both criminal expertise and cybercrime literature, particularly on the applicability of the criminal expertise framework to dark web pedophile forum users and provide a better understanding of the enculturation process among pedophile community.

1. Introduction

The nexus between criminology and technology was initially studied in an effort to understand how criminal activities translated to the online virtual world. This work is exemplified by Mann and Sutton (1998) Netcrime study on the theft of satellite signals. More recently, the nexus between criminology and technology has rapidly expanded to also encompass studies that use technologies to collect data on offenders (Décary-Hétu & Giommoni, 2017; Lee, Holt, & Smirnova, 2022; Péloquin, Fortin, & Paquette, 2022) and studies that investigate why and in what ways offenders are interested in technologies. History is replete with examples of new technologies that were put to use by offenders, ranging from using cars as getaway vehicles to the use of mobile phones to facilitate the illicit drug trade. Offenders adopt new technologies for manifold reasons, including, among other things, to enhance their security and anonymity online. This is evidenced by the creation of large anonymous online marketplaces on the dark web, which allow for large communities of people buying and selling illicit drugs to meet (Martin, Cunliffe, & Munksgaard, 2019). In this paper, we build on this line of research by investigating how sex offenders take advantage of communication technologies to enhance their skills and evade detection. The ability of individuals to avoid detection is consistent with the rational choice perspective (RCT) (Cornish & Clarke, 1986) which assumes that individuals rationalize their decision-making and behavioral processes to avoid the negative consequences they may suffer. While not all sex offenders are sufficiently sophisticated to utilize anonymity technologies (Chopin, Paquette, & Beauregard, 2022), those that do may share tips in their online forums about the strategies they have used over the course of their illicit activities. The acquisition of cyber security skills on the Internet has been described as a process of enculturation, being a part of the pedophile subculture (Holt, Blevins, & Burkert, 2010). One of the major challenges in studying the behavior of online sex offenders is the difficulty of reaching them. A potential solution is to adopt a method used in marketing research to study consumer behaviors. The principle of this method posits that the lifespan and survival of virtual contents are positively associated with the consumers' interest in the themes

* Corresponding author.
E-mail address: julienc@sfu.ca (J. Chopin).

https://doi.org/10.1016/j.jcrimjus.2023.102060
Received 1 February 2023; Received in revised form 13 March 2023; Accepted 17 March 2023
Available online 23 March 2023

addressed (Gonzalez & Palacios, 2004; Hernández, Jiménez, & Martín, 2009; Rekik, Kallel, Casillas, & Alimi, 2018). In this context, the aim of this study is to conduct an in-depth investigation on the use of cybersecurity strategies to prevent and counter threats by online sex offenders. The objectives of this study are to examine the lifespan and survival of threads extracted from pedophile forums on the darkweb, which are embedded in cybersecurity topics.

2. Cybersecurity expertise of online sex offenders: a rational choice approach

RCT provides a theoretical framework through which to analyze and understand the decision-making processes of offenders. This theoretical framework, which derives from economics, assumes that rationality and self-interest are foundational principles of criminal reasoning (Cornish, 1993; Cornish & Clarke, 1986; Piquero & Tibbetts, 2002). Assessing a situation based on a cost-benefit analysis is applicable both when an individual is not yet involved in a crime (i.e., the individual will engage in a crime only if they believe that the costs are less than the benefits) and when the individual is involved in the crime and must make the best decision to maximize the benefits and reduce the costs (Cornish, 1993; Cornish & Clarke, 1986). The decision-making and behavioral processes of individuals has historically been based on the articulation of two core concepts: 1) their ability to successfully carry out a crime, 2) their ability to avoid a range of threats such as detection and identification by the police (Nee, 2015; Nee & Taylor, 2000). On the one hand, the ability to successfully carry out a crime is highly dependent on the type of crime one is engaging in (e.g., sexual crimes, property crimes, etc.) and the motivation (e.g., for a sexual crime, several motivations can be involved, such as anger, sexual, sadism, etc.) for offenders to engage in it (Chopin, Paquette, & Beauregard, 2022). On the other hand, the ability to avoid threats (e.g., police detection, witness intervention) is a much more transversal concept that has been theorized under the idea of criminal expertise (Cherbonneau & Copes, 2005; Copes & Cherbonneau, 2006; Nee, 2015; Reale, Beauregard, & Chopin, 2021a, 2021b; Topalli, 2005; Ward, 1999). Although research in this area is long-standing (Sutherland, 1937), it is especially since the early 2000s that a series of studies focusing on different crime types (e.g., property, sexual, etc., Nee, 2015; Nee & Meenaghan, 2006; Nee et al., 2015; Reale, Beauregard, & Chopin, 2021c; Topalli, Jacques, & Wright, 2015; Ward, 1999) posited that, similarly to non-criminal contexts (e.g., chess players, pilot, Vicente & Wang, 1998), some individuals are more skilled than others when it comes to fulfilling certain tasks. Although this approach is ideologically controversial (Hirschi, 1986), empirical studies have shown that some individuals exhibit superior abilities to utilize certain strategies to avoid police detection than others. Moreover, individuals can also escape official sanctions for reasons completely out of their control, such as pure luck or inadequate investigative work (Rossmo, 2006, 2009 for more details). Although few studies have examined the subject, several results suggested that child sexual exploitation material (CSEM) offenders would not differ from offline sex offenders and would follow a rational decision-making process. Cohen-Almagor (2013) suggests that several goals may be pursued by CSEM offenders (i.e., collecting, sharing, trading) and that they use a number of strategies to avoid police detection. From a rational choice perspective, CSEM offenders try to limit the risks of being identified to maximize the benefits of their activities. Holt et al. (2010) identified security as one of the four major themes composing the pedophile subculture on the Internet. Several studies have empirically tested their ability to implement police avoidance strategies. For CSEM offenders, this requires the development of skills in assessing the risks they face and the methods they use to overcome them (Bourke, Ward, & Rose, 2012; Chopin, Paquette, & Fortin, 2022). Studies have shown that some individuals involved in online sexual crimes exhibit certain skills to avoid identification (Fortin & Paquette, 2018; Steel, Newman, O'Rourke, & Quayle, 2020). The initial question that drove these studies was to determine what techniques were employed by these individuals. A comprehensive literature review of the strategies utilized by CSEM offenders was published by Steel et al. (2020). They organized the different strategies according to their time period: the early network era (1987–1996), the internet era (1996–2004), the peer-to-peer era (2004–2008), the dark web era (2008–2014), and the mobile era (2014-present) (Steel et al., 2020). The two most recent time periods are the most relevant for this paper. The *dark web era* places the emphasis firmly on the anonymity that technology began to afford at that juncture, with Steel et al. (2020) citing numerous empirical studies related to this period (Acar, 2017; Chohan, 2017; Chopin, Paquette, & Fortin, 2022; Fortin, 2013; Krone et al., 2017; Loeb, 2017; McCarthy, 2010; Owen & Savage, 2015; Paquette & Fortin, 2021; Penna, Clark, & Mohay, 2005; Sanger & Chen, 2014; Steel et al., 2020). The Tor network and virtual private networks (VPN) were innovations that made it difficult for law enforcement to track who connected to what website or online resource. The use of cryptocurrencies like Bitcoin also made it possible to set up merchant websites where child abuse sexual material (CSEM) could be bought and sold. Estimates of the size of the population of pedophiles using the dark web vary greatly between tens of thousands to hundreds of thousands. In addition to anonymity technologies, the dark web era also saw the expansion of confidentiality technologies such as data encryption. This latter set of technologies prevent law enforcement from collecting evidence in the case of searches, and moreover, even affords plausible deniability insofar as an offender can appear to be collaborating with law enforcement when they are in fact still hiding illicit content on their hard drives. The *mobile era* places the emphasis on the use of mobile phones to both consume CSEM and communicate with other offenders. Instant-messaging applications like WhatsApp and Wickr as well as default messaging applications can be used to both share illicit content and set up video calls where victims are abused in real-time. Advances in mobile phone screen resolutions and internet speeds have made it possible for offenders to consume CSEM solely on their phones rather than on desktop or laptop computers.

The second focus of research on offenders and skills was to understand how individuals acquired the specific skills. One of the seminal studies on this issue was conducted by Holt et al. (2010). Grounded in a qualitative method, they provided evidence to support the existence of an online pedophile subculture through which individuals exchanged and acquired specific skills. Of the four main themes identified as defining the online pedophile subculture, two were devoted to issues of security and legal issues (Holt et al., 2010). This study opened the door to the hypothesis that skill acquisition can be achieved by deviant peers on specialized online exchange platforms such as pedophile forums. More recently, Chopin, Paquette, and Fortin (2022) analyzed the strategies used by online CSEM offenders, and identified two skill-building patterns in the strategies used to attempt to avoid police detection: 1) those that build on pre-existing knowledge, and 2) those that learn skills from their prior judicial experience. Those building on their pre-existing knowledge take advantage of posts and social connections to learn from the experience and discoveries of others, while those learning skills from their prior judicial experience study how law enforcement were able to identify them and collect evidence previously, and then change their behavior accordingly to prevent the same strategies from working again. This study confirms the transposability of results obtained with other crime types. Several studies examining the individuals involved in different types of offline sexual assaults (e.g., rape, sexual homicide) have also shown that a minority of these people were endowed with superior abilities to employ detection avoidance strategies (Beauregard & Bouchard, 2010; Beauregard & Martineau, 2014; Chopin, Beauregard, & Bitzer, 2020; Chopin, Beauregard, Bitzer, & Reale, 2019; Davies, 1992; Davies, Wittebrood, & Jackson, 1997; Stefanska & Carter, 2019). It is important to note here that several studies have stressed the difference between the use of avoidance strategies and their effectiveness in avoiding detection by police. The results of these studies indicate that for sexual assaults committed in an offline context, the strategies had

limited effect on avoiding detection and, in fact, may even be counterproductive in some circumstances (Beauregard & Martineau, 2014; Bitzer, Chopin, Beauregard, Mousseau, & Fortin, 2022; Chopin et al., 2019).

3. Life and death in the cyberspace

It is undeniable that an increasingly large part of criminal activity occurs either partly or wholly within a virtual environment (Caneppele & Aebi, 2019; Holt & Bossler, 2014). One of the major challenges in studying online offenders is the difficulty in reaching them. Criminological researchers have been inspired by e-consumer studies that aim to better understand customers' habits by studying their online behaviors. One of the key indicators of customer interest in online content is the lifespan of the content (Rekik et al., 2018; Robbins & Stylianou, 2003). The longer online content is active, the more it will be considered of interest to consumers. Research has demonstrated that accessibility, speed, navigability, and quality of content are the key factors that best predict the survival of legal online content (Gonzalez & Palacios, 2004; Hernández et al., 2009; Rekik et al., 2018). Westlake and Bouchard (2016) transposed this idea to examine which factors better predicted the survival of sites hosting CSEM. Based on the criminal career approach (Blumstein, Cohen, Das, & Moitra, 1988), they operationalized the four dimensions for online sites hosting CSEM in order to identify the best predictors of their lifespan (Westlake & Bouchard, 2016). This approach transposed studies focusing on the understanding of the desistance process among criminals (Paternoster, Bachman, Kerrison, O'connell, & Smith, 2016) and showed that both the volume of illegal content and the connectivity of websites were important predictors of website survival (Westlake & Bouchard, 2016). Specifically, the volume of illegal content was associated with sites' failure, insofar as it increased the visibility and risks of detection. Connectivity was associated with survival, insofar as the place that a website occupies in the overall network of CESM suppliers can serve to motivate its owners to maintain the website in operation (Westlake & Bouchard, 2016). Notwithstanding its innovative nature, this study confirms the idea that, similar to a non-criminal context, it is possible to analyze the behavior of online offenders via the virtual content they interact with.

4. Aim of the study

The literature review identified several important points. First, previous studies have shown that there exists a continuum of expertise among criminals, and that some of them are able to employ strategies to attempt to avoid external threats (e.g., police detection). Second, although limited, the literature nevertheless offers some evidence pertaining to the applicability of the criminal expertise framework for online sex offenders. Finally, previous studies have demonstrated that it is possible to improve our understanding of online offenders' behavior and decision-making processes by analyzing the content of the sites they use. While it is important to acknowledge that these studies have provided a better understanding of a hard-to-reach criminal population, there are several limitations associated with this body of knowledge. First, there is a dearth of studies examining the expertise of online sex offenders. Second, the empirical studies are primarily based on samples of individuals identified and arrested by the police (Chopin, Paquette, & Fortin, 2022), which limits the generalization of the results. Finally, studies of the cybersecurity strategies used by online sex offenders hitherto remain confined to technological considerations (Steel et al., 2020) or are primarily descriptive in nature (Paquette & Fortin, 2021). In this context, our understanding of how online sex offenders protect themselves against the risk of detection and arrest remains limited. Given the profound harm that these offenders create, it is particularly essential to study and model how online sex offenders use online security techniques. Although these individuals are a hard-to-reach population, adopting an indirect approach to study this problem might yield results. As Holt et al. (2010) demonstrated, online discussion forums can be rich sources of data on online sex offenders. Indeed, these forums provide many valuable data points, such as, for example, the lifespan and survival of discussion threads devoted to online security. Such an approach identifies individuals' interests in online security and highlights the preferred mechanisms through which to achieve a higher level of security. Specifically, this study proposes to answer two research questions:

RQ1. Are there any cybersecurity topics that predict the lifespan of discussion threads?'

RQ2. Are there any cybersecurity topics that predict the survival of discussion threads?

5. Methods

5.1. Data and sample

The data used in this research was collected as part of the *Anonymity, technology and crime: Hiding in the shadows* (SSHRC. Insights #435-2018-1060) project. The objective of this research program was to better understand the use of strategies by online offenders to avoid police detection and identification. The data was collected from three pedophile forums identified on the dark web in which we identified threads that specifically focused on cybersecurity topics. The sample analyzed consists of 290 cybersecurity-related threads. To identify pedophile forums dealing with security issues, the following keywords were combined: boy lover, girl lover, child lover, pedophiles, pedophilia, forums, security, law enforcement, online security, encryption, Freenet, TOR, and police. These threads represent a total of 10,134 messages that were posted between May 11, 2009, and July 3, 2022 (the date of data collection). The selection of these three forums was made on the basis of two criteria: 1) sufficiently detailed discussions on technology-related themes, 2) forums dealing with the dark web and mobile digital eras (i.e., 2008-present; Steel et al., 2020). The information was collected in text form and coded in a database. The coding of the data was performed by two research assistants who were specifically trained for this purpose. Approximately 10% of the threads and messages were selected to assess the inter-rater reliability. Overall, the agreement on coding reached 96.5% ($\kappa = 0.919$). Each thread had an average number of 35 messages that were supplied on average by nine different users. At the time of extraction (i.e., July 3, 2022) each thread had been viewed on average 16,796 times and was created on average 518 days before the data were collected.

5.2. Measures

5.2.1. Dependent variables

In order to measure the lifespan of the threads, we used several dependent variables. The first dependent variable, the length of the thread activity in terms of days, is continuous and was created by subtracting the date of the first message from the date of the last message posted on the thread ($\bar{X} = 517.66$ days, $SD = 869.62$, range 1–4259). This variable was non-normally distributed with a skewness of 2.05 ($SE = 0.14$) and a kurtosis of 3.62 ($SE = 0.29$). The second dependent variable is dichotomous and allowed us to distinguish between the threads that were still active and those that were no longer active (0 = inactive; 1 = active). In order to operationalize the inactivity of a thread, also called 'death' in survival analysis, we had to consider a sufficient period of inactivity. Studies examining the lifespan of virtual content have shown that after a period of inactivity (i.e., no messages posted) between 3 and 6 months, the virtual content could be considered as 'dead' (Wang, Guo, & Chen, 2016; Yang, Wei, Ackerman, & Adamic, 2010). In order to be as conservative as possible and to limit the possibility of false positives, we chose the longer time period (i.e., 6 months) as an indication of 'death' in our analysis. For example, we considered threads that had no

messages posted in the six-month period prior to the date of the data extraction to be inactive (i.e., July 3, 2022). In order to avoid introducing bias in the analysis, we excluded seven threads created during the 6 months before the extraction date. The survival analyses were therefore performed with a sample of 283 threads.

5.2.2. Independent variables

Previous studies have shown that online sexual offenders were able to protect themselves from external threats by using different proactive and/or reactive strategies (Chopin, Paquette, & Fortin, 2022; Paquette & Fortin, 2021; Steel et al., 2020). We used a total of 27 dichotomous variables (0 = absence; 1 = presence) to characterize the cybersecurity topics discussed on the forums. These variables allowed us to operationalize eight different themes related to cybersecurity issues: Protection against external threats, avoiding localization, avoiding identification, refraining from using certain risky technologies, online search without leaving traces, criminal activities and law enforcement, strategies for obstructing justice, and the level of expertise present in the threads. The first two variables are related to protection against cyber threats: 1) malware prevention and 2) malware identification. The following variables are related to localization avoidance: 3) use of proxy, 4) anonymizing service, 5) traffic encryption. Then, we used five additional variables related to identification avoidance: 6) use of prepaid services, 7) use of cryptocurrency, 8) use of false documents, 9) creating a new identity, 10) use of public WIFI only. Two more variables allowed us to operationalize refraining from using certain risky technologies: 11) use of a cell phone only, 12) avoiding using cloud data hosting. To characterize strategies that allow for searching online without leaving traces, five variables were used: 13) search engine, 14) cookies, 15) browsers, 16) flash player, 17) social networks. In order to test the level of interest in the topics related to criminal activities and law enforcement, we used the following variables: 18) risk factors for law enforcement identification, 19) legal consequences of online criminal activity. With respect to the strategies for obstructing justice, we used five additional variables: 20) anonymous operating systems, 21) regular destruction of data, metadata, 22) emergency data destruction, 23) communication encryption, 24) hard-drive encryption. Finally, according to the criminal expertise perspective, individuals do not all have the same skills and ability to use police avoidance strategies (Nee & Ward, 2015). In order to determine the level of expertise associated with the different cybersecurity topics, we used three variables. These variables assess the level of expertise within each thread: 25) low level of expertise (i.e., basic questions), 26) medium level of expertise (i.e., asking questions and seeking support, slightly advanced basic knowledge), and 27) expert level of expertise (i.e., understands how anonymity/security technologies work and can explain it, share knowledge with other members at a lower level than themselves). It is important to note that these three variables are not mutually exclusive since they characterize the level of expertise of the messages present in the threads. It is therefore quite likely that a thread is composed of messages with different levels of expertise.

5.3. Analytical strategy

The goal of this study was to determine which cybersecurity themes were associated with threads' lifespan and survival, and, to this end, we followed a two-step analytical process. The first analytical step consisted of bivariate comparisons. The goal here was to identify at the bivariate level the factors that were associated with both the length of the thread activity (i.e., Mann-Whitney U[1]) and the survival of the thread (Mantel–Cox test). The second analytical step included two multivariate analyses using only independent variables that were significant at the bivariate level (Hosmer & Lemeshow, 2013). Specifically, one sequential generalized linear model (GLM) with negative binomial log function[2] (Nelder & Wedderburn, 1972), and one Cox proportional hazard regression model (Cox, 1972) were computed. The sequential GLM with negative binomial log function was carried out to better understand the impact of each block of independent variables. Next, a nested binomial regression analysis was conducted using only the significant variables from all the previous models, which represented the final and best model. The Cox proportional hazard regression model was used to relate several independent variables, which were considered simultaneously, to survival time. In a Cox proportional hazards regression model, the measure of effect is the hazard rate, which is the risk of failure (i.e., the risk or probability of suffering the event of interest), given that the statistical unit has survived up to a specific time. A probability must lie within the range of 0 to 1. However, the hazard represents the expected number of events per one unit of time. Multicollinearity was checked for the variables included in the multivariate analyses; no variance inflation factors (VIFs) were above 2.64, and the tolerance was not below 0.34 (Appendix 1).

6. Results

Bivariate analyses were conducted between the independent and dependent variables. Table 1 shows that 12 independent variables were significantly associated with the length of the thread activity dependent variable. The findings show that topics related to malware prevention (Mann-Whitney U = 2258; $p < .001$), malware identification (Mann-Whitney U = 2264.50; $p = .018$), the use of a proxy (Mann-Whitney U = 7140.50; $p < .001$), traffic encryption (Mann-Whitney U = 3122.50; $p < .001$) and the use of a cell phone only (Mann-Whitney U = 872; $p = .015$) were significantly associated with the length of the thread activity. Moreover, discussion related to risk factors for law enforcement identification (Mann-Whitney U = 3100.50; $p < .001$), the legal consequences of online criminal activity (Mann-Whitney U = 886.50; $p < .001$), the use of anonymous operating systems (Mann-Whitney U = 2898.50; $p = .021$), the regular destruction of data and metadata (Mann-Whitney U = 2476.50; $p = .019$) and communication encryption (Mann-Whitney U = 5205; $p < .001$) were significantly associated with the length of the thread activity. Finally, the length of the thread activity was significantly associated with the presence of medium (Mann-Whitney U = 7788.50; $p = .023$) or expert (Mann-Whitney U = 5288; $p = .001$) level of competency in the topics discussed.

Regarding the factors that were associated with threads' survival, the results show that topics related to malware identification (log rank $\chi^2 = 8.61$; $p = .003$), the use of a proxy (log rank $\chi^2 = 18.08$; $p < .001$), traffic encryption (log rank $\chi^2 = 9.99$; $p = .002$), the use of prepaid services (log rank $\chi^2 = 8.51$; $p = .004$) were significantly associated with threads' survival. Moreover, topics such as risk factors for law enforcement identification (log rank $\chi^2 = 15.19$; $p < .001$) and hard-drive encryption (log rank $\chi^2 = 5.85$; $p = .016$) were significantly associated with threads' survival. Finally, the presence of medium (log rank $\chi^2 = 14.73$; $p < .001$) or expert (log rank $\chi^2 = 7.06$; $p = .008$) level of discussion in a thread was significantly associated with its survival.

Table 2 describes the results of the sequential GLM with negative binomial log function of factors predicting threads' lifespan. A total of seven distinct models (i.e., six sequenced models, and one nested model) were computed. Model 1 includes only the protection against external threats-related topics and presents an AIC of 4176. The results show that threads discussing malware prevention ($\beta = 0.92$, $p < .001$) and malware identification ($\beta = 0.54$, $p = .011$) were more likely to have a longer activity length. Model 2 includes only the avoidance localization-related topics and presents an AIC of 4161. The findings show that

[1] A Mann-Whitney U nonparametric test was used as the dependent variable did not follow a normal distribution.

[2] This parameter was used because the dependent variable followed a negative binomial distribution.

Table 1
Bivariate analysis of the factors predicting threads' lifespan and survival.

	Total	Thread lifespan (N = 290)		Thread survival (N = 283)	
	n = (%)	Mann-Whitney U	*p*-Value	Log-rank (Mantel-Cox)	p-Value
Protection against external threats					
Malware Prevention	29 (10.00)	2258.00	<0.001	2.78	0.096
Malware Identification	24 (8.27)	2264.50	0.018	8.61	0.003
Avoiding localization					
Proxy	130 (44.82)	7140.50	<0.001	18.08	<0.001
Anonymizing service	19 (6.55)	2077.50	0.158	1.38	0.241
Traffic encryption	38 (13.10)	3122.50	<0.001	9.99	0.002
Avoiding identification					
Use of prepaid services	11 (3.79)	1188.00	0.202	8.51	0.004
Use of cryptocurrency	8 (2.75)	815.00	0.179	2.72	0.187
Use of false documents	3 (1.03)	347.50	0.564	1.53	0.216
Creating a new identity	7 (2.41)	804.50	0.394	0.04	0.852
Public WIFI only	7 (2.41)	630.00	0.098	1.60	0.206
Refraining from using certain risky technologies					
Use of cell phone only	11 (3.79)	872.00	0.015	1.65	0.203
Cloud data hosting	2 (0.68)	265.50	0.848	0.52	0.473
Online search without leaving traces					
Search engine	27 (9.31)	3355.00	0.636	1.74	0.473
Cookies	16 (5.51)	1698.00	0.128	2.00	0.157
Browsers	1 (0.34)	107.00	0.745	0.01	0.944
Flash Player	5 (1.72)	389.00	0.080	2.03	0.154
Social networks	7 (2.41)	706.50	0.193	0.06	0.807
Criminal activities and law enforcement					
Risk factors for law enforcement identification	38 (13.10)	3100.50	<0.001	15.19	<0.001
Legal consequences of online criminal activity	15 (5.17)	886.50	<0.001	4.79	0.109
Strategies for obstructing justice					
Anonymous operating systems	30 (10.34)	2898.50	0.021	3.08	0.079
Regular destruction of data, metadata	26 (8.96)	2476.50	0.019	3.61	0.060
Emergency data destruction	1 (0.34)	7000.00	0.055	3.19	0.074
Communication encryption	64 (22.06)	5205.00	<0.001	3.31	0.070
Hard disk encryption	78 (26.89)	7191.50	0.088	5.85	0.016
Level of expertise present in threads					
Level of expertise: Low	214 (73.79)	7260.00	0.163	0.88	0.347
Level of expertise: Medium	227 (78.27)	7788.50	0.023	14.73	<0.001
Level of expertise: Expert	96 (33.10)	5288.00	0.001	7.06	0.008

threads discussing the use of a proxy (β = 0.64, p < .001) as well as traffic encryption (β = 0.44, p = .020) were more likely to have a longer activity length. Model 3 includes only the refraining from using certain risky technologies-related topics and presents an AIC of 4195. The results indicate that threads discussing the use of a cell phone only (β = 0.99, p = .001) were more likely to have a longer activity length. Model 4 includes only the criminal activities and law enforcement-related topics and presents an AIC of 4154. Threads discussing risk factors for law enforcement identification (β = 0.80, p < .001) and legal consequences of online criminal activity (β = 1.05, p < .001) were more likely to have a longer activity length. Model 5 includes only the strategies for obstructing justice-related topics and presents an AIC of 4182. Threads where anonymous operating systems (β = 0.46, p = .018), regular destruction of data/metadata (β = 0.63, p = .002), and communication encryption (β = 0.50, p < .001) were discussed were more likely to have a longer activity length. Model 6 includes only the variables related to the level of expertise present in the threads and presents an AIC of 4193. Those threads characterized by an expert level of competencies were more likely to have a longer activity length. Finally, the parsimonious model includes only the significant variables from the previous models and presents an AIC of 4115. Threads discussing malware prevention (β = 0.50, p = .022), use of a proxy (β = 0.43, p = .002), risk factors for law enforcement identification (β = 0.76, p < .001), and legal consequences of online criminal activity (β = 0.98, p < .001) were more likely to have a longer activity length. The result related to the control variable suggests that those threads with longer activity length (β = 1.11, p < .001) were more likely to survive, as was the case for all other models.

Fig. 1 describes the Kaplan-Meier estimated probability of threads' survival. The Kaplan-Meier function indicates that after a few days of activity, several threads came to an end. Only a limited number of threads were able to remain active for a long-time span with a maximum of 4254 days (i.e., eleven years, seven months, twenty-four days).

Table 3 presents the results of the Cox proportional hazard regression model of the factors predicting threads' survival. The log-likelihood ratio test is significant (p < .001), suggesting that taken together, the variables included in the model affect threads' survival time. The findings suggest that the presence of topics related to the use of a proxy (HR[3] = 0.67; p = .005) and to risk factors for law enforcement identification (HR = 0.56; p = .005) increase the likelihood of a thread's survival by 1.49 times and 1.78 times, respectively. Moreover, the presence of medium (HR = 0.96; p = .042) and expert (HR = 0.86; p = .029) competency levels increases the likelihood of a thread's survival by 1.04 times and 1.16 times, respectively.

7. Discussion

This study aimed to improve knowledge related to online sex offenders' online security concerns. In order to achieve this goal, this research was framed within the criminal expertise approach, an extension of RCT, in order to understand individuals' cybersecurity strategies. Based on e-commerce studies (Gonzalez & Palacios, 2004; Hernández et al., 2009; Rekik et al., 2018) that have been effectively applied to the field of criminology by Westlake and Bouchard (2016), the approach we followed consisted of analyzing the cybersecurity themes that predicted both the lifespan and survival of the related threads. As is the case in e-commerce studies, this research is predicated on the notion that the content of a digital entity influences the interest of its users and thus its lifespan (Rekik et al., 2018; Robbins & Stylianou, 2003).

First, the results suggest that there is a hierarchy with respect to predicting threads' lifespan between the different types of content that have been analyzed. Indeed, if we accept the idea that a thread's lifespan reflects the interest of its users, then those that receive the most attention are: criminal activities and law enforcement > localization

[3] Hazard Ratio

Table 2
Sequential generalized linear model with negative binomial log function of the factors predicting threads' lifespan (N = 290).

	Model 1		Model 2		Model 3		Model 4		Model 5		Model 6		Best Model	
	β	SE	β	SE	β	SE	β	SE	β	SE	β	SE	β	SE
Constant	6.05***	0.06	5.81***	0.08	6.18***	0.06	5.99***	0.06	5.979***	0.07	5.86	0.13	5.51***	0.09
Protection against external threats														
Malware Prevention	0.92***	0.20											0.50*	0.22
Malware Identification	0.54*	0.21											0.29	0.23
Avoid localization														
Proxy			0.64***	0.13									0.43**	0.14
Traffic encryption			0.44*	0.19									0.25	0.21
Refraining from using certain risky technologies														
Use of cell phone only					0.99**	0.31							−0.31	0.35
Criminal activities and law enforcement														
Risk factors for law enforcement identification							0.80***	0.18					0.76***	0.19
Legal consequences of online criminal activity							1.05***	0.27					0.98***	0.29
Strategies for obstructing justice														
Anonymous operating systems									0.46*	0.19			0.11	0.21
Regular destruction of data. Metadata									0.63**	0.21			0.39	0.23
Communication encryption									0.50***	0.14			0.47	0.16
Level of expertise present in threads														
Level of expertise: Medium											0.29	0.15		
Level of expertise: Expert											0.39**	0.13	−0.16	0.15
Control variable														
Threads' survival	1.05***	0.06	0.89***	0.23	1.05***	0.22	1.09***	0.22	1.14***	0.22	−0.53	0.37	1.11***	0.24
Deviance	1309.54		1294.57		1330.05		1287.45		1313.02		1326.43		1230.64	
Pearson χ^2	837.03		907.64		817.53		822.38		857.16		792.44		950.53	
Scaled Pearson χ^2	837.03		907.64		817.53		822.38		857.16		792.44		950.53	
Log Likelihood	−2085.16		−2077.67		−2095.41		−2074.11		−2086.90		−2093.60		−2045.71	
Akaike's Information Criteria (AIC)	4176.32		4161.34		4194.83		4154.22		4181.79		4193.20		4115.41	
Finite Sample Corrected AIC (AICC)	4176.40		4161.43		4194.87		4154.31		4181.93		4193.28		4116.54	
Baysian Information Criterion (BIC)	4187.33		4172.35		4202.17		4165.23		4196.47		4204.21		4159.45	
Consistent AIC (CAIC)	4190.33		4175.35		4204.17		4168.23		4200.47		4207.21		4171.45	

Notes. *$p < .05$. **$p < .01$. ***$p < .001$.

avoidance > protection against external threats> strategies for obstructing justice > refraining from using some specific technology. It is interesting to note that two dimensions appear to interfere with this, namely: the *level of abstraction of the content* and the *temporality of the strategy use*. The findings suggest that content with the highest level of abstraction and the lowest level of computer skills are connected with threads' lifespan and survival. In particular, content discussing risk factors related to police detection is the best predictor for both threads' lifespan and survival. Such a result is congruent with the very idea of the expertise principle (i.e., in a criminal context or otherwise), which posits that the skills with the highest level of specialization are also those that have the smallest number of individuals who are aware of their existence and interested in them (Chopin, Paquette, & Beauregard, 2022; Nee & Ward, 2015; Vicente & Wang, 1998). Considering the criminal expertise perspective which assumes the existence of a pyramidal distribution of the individuals' skills (Reale, 2022), the topics with the lowest complexity level could be the ones that hold the attention of the greatest number of them. Moreover, it appears reasonable to suggest that prior to looking at specific techniques, users should be aware of and learn about the risk factors that might lead them to use these strategies. The temporality concept is also important when distinguishing between proactive and reactive strategies (Fortin & Paquette, 2018). Our study shows that strategies to avoid localization as well as strategies to protect against external threats are better predictors than strategies to obstruct the judiciary process. Consequently, we can hypothesize that the users of the pedophile forums we analyzed do not wait to be confronted with the police before reacting, but rather engage in proactive protection techniques. Although no study has previously examined this, these results could be different if one were to use a sample of individuals identified by the police who may have neglected this step of proactive protection. These results illustrate the concept of bounded rationality developed in the RCT (Cornish & Clarke, 1986; Cornish & Clarke, 1987; Gigerenzer & Selten, 2002). Indeed, we observe that if all individuals are concerned by cybersecurity issues and the will to limit risks, the level of sophistication

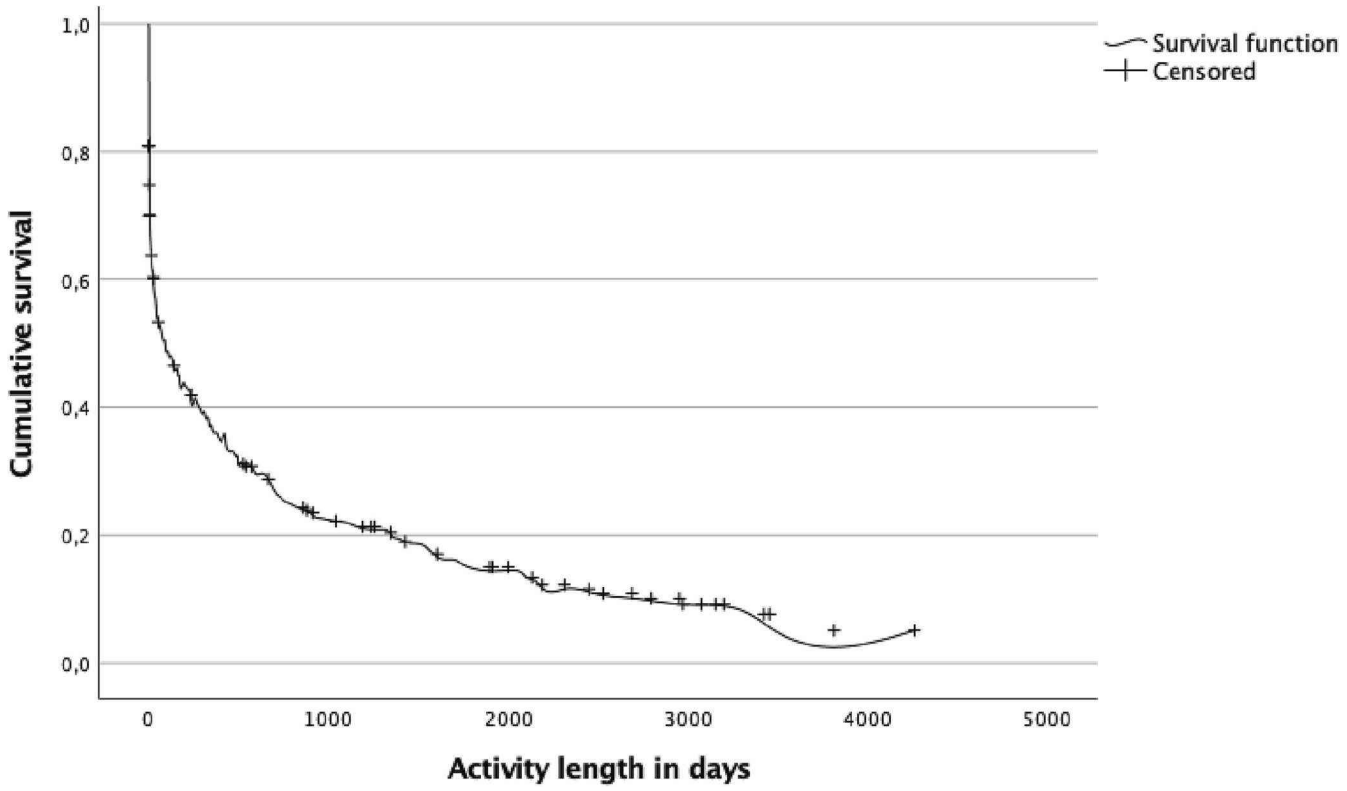


Fig. 1. Kaplan-Meier survival function: Estimated probability of threads' survival (N = 283).

Table 3
Cox proportional hazard regression model of the factors predicting threads' survival (N = 283).

	β	SE	Hazard ratio	95% CI Hazard ratio	
Protection against external threats					
Malware Identification	−0.19	0.23	0.83	0.52	1.31
Avoiding localization					
Proxy	−0.40**	0.14	0.67	0.51	0.89
Traffic encryption	−0.17	0.21	0.84	0.56	1.27
Avoiding identification					
Use of prepaid services	−0.47	0.41	0.63	0.28	1.41
Criminal activities and law enforcement					
Risk factors for law enforcement identification	−0.58**	0.20	0.56	0.38	0.84
Strategies for obstructing justice					
Hard-drive encryption	−0.03	0.15	0.99	0.74	1.34
Level of expertise present in threads					
Level of expertise: Medium	−0.05*	0.16*	0.96	0.92	0.98
Level of expertise: Expert	−0.16*	0.15*	0.85	0.77	0.95
Log-likelihood ratio test	2555.12*** (df = 8)				
−log2(p) of ll-ratio test	2517.19				

Notes. *$p < .05$. **$p < .01$.

in the distribution of the topics varies widely. The rational subjectivity observed in the decision-making process to be interested in and to implement more sophisticated techniques could be dependent on the individual's skills and knowledge (Nee & Ward, 2015). Second, it is possible that the lifespan of a thread could have been negatively associated with its survival. In other words, those threads that were still active could have been those that were created most recently. However, the analyses show a positive association between the active status of threads and their lifespan. This result is interesting because it suggests that the threads that were still active were those with the longest lifespan. Therefore, such a result suggests that certain threads have sufficiently relevant content that allows them to remain active over time and generate frequent activity. The survival function complements this analysis by revealing that most threads failed after a short period of time, while a minority of them survived for a significant period of time. Third, beyond the convergences between the lifespan and survival analyses, divergences must also be addressed. We note that, contrary to the model predicting lifespan, the topics related to protection against external threats are not significant in the survival analysis. Although we do not have a definitive answer for why this is the case, we hypothesize that external threats are constantly evolving over time (i.e., new malware and computer viruses are regularly identified) and that the technologies to counter them are thus also highly evolving (Gupta, Kuppili, Akella, & Barford, 2009). Given these regular changes, it is possible that these topics do not allow such a theme to survive over time. We can also hypothesize that users of these forums focus their interest on police avoidance strategies rather than other computer threats. From a RCT perspective, this could suggest a prioritization of threats in the risk assessment made by individuals. In other words, individuals' decision-making could be influenced by threats, and the focus of managing those threats are perceived to be the most important. We could also consider that although computer threats were once considered to be a major risk, which is why this theme is significant in predicting threads' lifespan, IT development has subsequently relegated them to minor threats (Alenezi, Alabdulrazzaq, Alshaher, & Alkharang, 2020). Finally, we observe that the level of expertise perceived by users is an important predictor of threads' survival. Thus, threads whose discussions have a medium and expert level of competency are more likely to survive. These results are congruent with Holt et al. (2010) study, who highlighted the existence of a pedophile subculture on online platforms and

found that security-related skills were exchanged. Consequently, we put forward the hypothesis that those threads that allow users to improve their level of skill and knowledge are valued and fed with more content (e.g., questions from novices to expert users). It is also possible that a small number of threads are the privileged discussion vectors of groups designated as expert users by the community, and that they are therefore used much more than others. This finding echoes the results of studies suggesting that the quality of content is a key factor in predicting the survival of legal and illegal online content (Gonzalez & Palacios, 2004; Hernández et al., 2009; Rekik et al., 2018; Westlake & Bouchard, 2016).

8. Conclusion

This research focused on the cybersecurity concerns of dark web pedophile forum users. In order to study this hard-to-reach population, we developed an innovative methodology inspired by studies on e-commerce consumers that have recently been transposed to criminology. Based on the notion that both the lifespan and survival of virtual content are associated with the interest of users, we analyzed the predictors of these two measures among a sample of threads related to cyber security that were imported from three dark web pedophile forums. This study, which was framed by a criminal expertise approach, identified a number of interesting and novel findings. First, our results showed that risk factors for law enforcement identification-related topics were the most predictive of threads' lifespan and survival. Second, topics related to proactive protection strategies were more predictive than those related to reactive ones. Third, the analyses showed that the thread survival is positively associated with its life span suggesting that some threads survive for a significant period of time because they contain relevant content that is of interest to users. Finally, threads with a superior skill level was more likely to survive than other types of content.

This research has several implications. Theoretically speaking, this research confirms the applicability of the RCT and criminal expertise framework to dark web pedophile forum users. The results reflect the existence of a pyramidal pattern of expertise in which the majority of users are interested in themes with a high level of abstraction (i.e., risk factors for law enforcement identification), while a minority are interested in specific strategies (e.g., emergency data destruction, use of cryptocurrency). Moreover, this study highlights the presence of a certain degree of awareness of the risks involved, insofar as the preferred techniques are proactive, thus suggesting a sense of anticipation from users. More generally, these findings add to extant literature on pedophile subcultures by confirming that novices learn from experts on virtual platforms. This pattern of peer-based skill acquisition appears to be specific to online crime and has not been identified in prior studies examining the expertise of offline sex offenders. Finally, this study confirms the transposability of methods from other disciplines (i.e., e-commerce) to study online sex offenders' behaviors via the identification of common patterns (e.g., quality of content). With respect to the practical implications, this research indicates that dark web pedophile forums are not likely to be interested in sophisticated strategies to protect themselves beyond that of hiding their identity. This, in turn, suggests that law enforcement agencies should focus their efforts on developing protocols to counter these particular strategies. In addition, this study demonstrates that monitoring the virtual spaces in which criminals congregate can provide interesting intelligence through which to better understand the criminal behavior of individuals. Such intelligence work could be developed at an operational level to better understand the behavior of individuals who are being investigated. As to the policy implications, the most effective measures may be to work with (and not against) the Dark Web to de-anonymize content (Davis & Arrigo, 2021). Several programs aim to reduce the anonymity and sense of impunity that prevails among Dark Web users. For example, the Memex program (from the Defense Advanced Research Projects Agency) aims to combat this issue by referencing and indexing the content of the Dark Web in order to have a better idea of how the information is circulating (Davis & Arrigo, 2021). Such an approach could have the effect of deterring some individuals from sharing information and undermining the operating structure of the pedophile subculture on the Internet.

Although this study provides several new findings, it is not without its limitations. First, we must acknowledge that our findings could be affected by a selection bias. This concerns the fact that the sample that was analyzed pertained to threads exclusively devoted to cybersecurity. This implies that the users of these threads are individuals with a manifest interest in this issue, and we cannot exclude that the patterns of expertise might have been different if we had considered all users who frequent pedophile forums. Moreover, these forums are hosted on the dark web, which implies that the individuals who access them already possess a minimal level of competency. This selection bias implies a likely overestimation in our results of the actual cybersecurity level of all pedophile forum users. Second, the underlying idea of thread inactivity is that users lost interest in the topics being discussed. However, we have no way of verifying whether this was in fact the case, and, hence, we cannot exclude that thread inactivity might have been related to other reasons (e.g., arrest of main users, moderation by the forum administrator, etc.). Third, we decided to operationalize the thread activity/inactivity using an arbitrary measure of 6 months or more without any posts at the date of the data extraction. We cannot exclude the possibility that the day after the extraction was completed a post was made, thus rendering our measure irrelevant. Fourth, only users (i.e., those who feed the discussion) were used to operationalize the thread activity. Another option would have been to also consider the number of views of the thread as being indicative of activity. Unfortunately, it was not possible to collect detailed and time-stamped data of the views on each thread. An operationalization combining views with user activities could have changed the results of our study by reducing the number of inactive threads. Fifth, one of the measures used in this study is the level of expertise of the messages contained in the different threads. This measure was evaluated by the persons who coded information and it is possible that there are discrepancies in the assessment made. However, the level of inter-rater agreement is sufficiently high to consider that these risks are limited. Finally, the cybersecurity themes were analyzed over a 13-year period. Although the variables used are sufficiently broad enough to avoid the specificity any particular technology, we cannot exclude that some of them were influenced by the appearance or disappearance of particular threats during the analysis period. Furthermore, we cannot exclude that certain cybersecurity themes are more or less present across this time window, depending on technological developments.

Future studies should expand our knowledge of illegal digital content and their lifespan and survival. Such studies would confirm the expedience of the method and challenge the results proposed in this study. In addition, future studies should extend the methodological approach by trying to obtain a more representative sample than we included in this study. One goal would be to complement the approach delineated here by understanding why some individuals use strategies while others do not, which could be ascertained via an online survey disseminated on pedophile websites. Finally, it would be interesting to determine if the use of strategies is a hindrance to police work or if it in fact has little impact on the investigations conducted, as is the case for sex crimes carried out offline.

Appendix A. Appendix

Appendix 1
Multicollinearity diagnosis.

	Model 1[a]		Model 2[b]	
	Tolerance	VIF	Tolerance	VIF
Malware Prevention	0.39	2.57	–	–
Malware Identification	0.38	2.64	0.94	1.07
Proxy	0.75	1.34	0.81	1.23
Traffic encryption	0.80	1.25	0.83	1.21
Use of prepaid services	–	–	0.92	1.09
Use of cell phone only	0.91	1.10	–	–
Risk factors for law enforcement identification	0.91	1.10	0.91	1.10
Legal consequences of online criminal activity	0.86	1.16	–	–
Anonymous operating systems	0.83	1.21	–	–
Regular destruction of data, metadata	0.94	1.07	–	–
Communication encryption	0.92	1.09	–	–
Hard disk encryption	–	–	0.88	1.14
Level of expertise: Medium	0.84	1.20	0.83	1.20
Level of expertise: Expert	0.84	1.20	0.85	1.18

[a] Corresponds to the Sequential negative binomial generalized linear model.
[b] Corresponds to the Cox Proportional Hazard Regression Model.

References

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

Alenezi, M. N., Alabdulrazzaq, H., Alshaher, A. A., & Alkharang, M. M. (2020). Evolution of malware threats and techniques: A review. *International journal of communication networks and information security, 12*(3), 326–337.

Beauregard, E., & 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

Beauregard, E., & Martineau, M. (2014). No body, no crime? The role of forensic awareness in avoiding police detection in cases of sexual homicide. *Journal of Criminal Justice, 42*(2), 213–220. https://doi.org/10.1016/j.jcrimjus.2013.06.007

Bitzer, S., Chopin, J., Beauregard, E., Mousseau, V., & Fortin, F. (2022). Sexual homicide and the forensic process: The decision-making process of collecting and analyzing traces and its implication for crime solving. *Forensic Science International, 340*, Article 111446. https://doi.org/10.1016/j.forsciint.2022.111446

Blumstein, A., Cohen, J., Das, S., & Moitra, S. D. (1988). Specialization and seriousness during adult criminal careers. *Journal of Quantitative Criminology, 4*(4), 303–345.

Bourke, P., Ward, T., & Rose, C. (2012). Expertise and sexual offending: A preliminary empirical model. *Journal of Interpersonal Violence, 27*(12), 2391–2414.

Caneppele, S., & 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., & 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., Beauregard, E., & Bitzer, S. (2020). Factors influencing the use of forensic awareness strategies in sexual homicide. *Journal of Criminal Justice, 71*, 1–9. https://doi.org/10.1016/j.jcrimjus.2020.101709

Chopin, J., Beauregard, E., Bitzer, S., & Reale, K. (2019). Rapists' behaviors to avoid police detection. *Journal of Criminal Justice, 61*(2019), 81–89. https://doi.org/10.1016/j.jcrimjus.2019.04.001

Chopin, J., Paquette, S., & Beauregard, E. (2022). Is there an expert stranger "rapist". *Sexual Abuse, 34*(1). https://doi.org/10.1177/1079063221993478

Chopin, J., Paquette, S., & 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

Cohen-Almagor, R. (2013). Online child sex offenders: Challenges and counter-measures. *The Howard Journal of Criminal Justice, 52*(2), 190–215.

Copes, H., & 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. (1993). Theories of action in criminology: Learning theory and rational choice approaches. In R. V. Clarke, & M. Felson (Eds.), *Routine activity and rational choice* (pp. 351–382). Transaction.

Cornish, D. B., & Clarke, R. V. (1986). Introduction. In D. B. Cornish, & R. V. Clarke (Eds.), *The reasoning criminal: Rational choice perspectives on offending* (pp. 1–18). Springer-Verlag.

Cornish, D. B., & Clarke, R. V. (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

Cox, D. R. (1972). Regression models and life-tables. *Journal of the Royal Statistical Society: Series B: Methodological, 34*(2), 187–202. https://doi.org/10.1111/j.2517-6161.1972.tb00899.x

Davies, A. (1992). Rapists' behaviour: A three aspect model as a basis for analysis and the identification of serial crime. *Forensic Science International, 55*(2), 173–194. https://doi.org/10.1016/0379-0738(92)90122-D

Davies, A., Wittebrood, K., & 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

Davis, S., & Arrigo, B. (2021). The dark web and anonymizing technologies: Legal pitfalls, ethical prospects, and policy directions from radical criminology. *Crime, Law and Social Change, 76*(4), 367–386.

Décary-Hétu, D., & Giommoni, L. (2017). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of operation Onymous. *Crime, Law and Social Change, 67*(1), 55–75. https://doi.org/10.1007/s10611-016-9644-4

Fortin, F. (2013). Usenet newsgroups, child pornography, and the role of participants. In C. Morselli (Ed.), *Crime and networks* (1st ed.). Routledge.

Fortin, F., & Paquette, S. (2018). Online sexual exploitation of children: Reactive and proactive policing. In P. Lussier, & S. Paquette (Eds.), *Sexual offending: A criminological perspective* (pp. 237–256). Routledge.

Gigerenzer, G., & Selten, R. (2002). *Bounded rationality: The adaptive toolbox*. MIT press.

Gonzalez, F. M., & 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

Gupta, A., Kuppili, P., Akella, A., & Barford, P. (2009). An empirical study of malware evolution. In *2009 first international communication systems and networks and workshops*.

Hernández, B., Jiménez, J., & 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

Hirschi, T. (1986). On the compatibility of rational choice and social controltheories of crime. In D. B. Cornish, & R. V. Clarke (Eds.), *The reasoning criminal* (pp. 105–118). Springer-Verlag.

Holt, T. J., Blevins, K. R., & Burkert, N. (2010). Considering the pedophile subculture online. *Sexual Abuse, 22*(1), 3–24. https://doi.org/10.1177/1079063209344979

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35*(1), 20–40. https://doi.org/10.1080/01639625.2013.822209

Hosmer, D. W., & Lemeshow, S. (2013). *Applied logistic regression* (2nd ed.). John Wiley & Sons.

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

Lee, J. R., Holt, T. J., & Smirnova, O. (2022). An assessment of the state of firearm sales on the dark web. *Journal of Crime and Justice, 1-15*. https://doi.org/10.1080/0735648X.2022.2058062

Loeb, J. (2017). Europol study assesses technology for fighting online child abuse [news briefing]. *Engineering and Technology, 12*(10), 8. https://doi.org/10.1049/et.2017.1011

Mann, D., & Sutton, M. (1998). >> NETCRIME: More change in the organization of thieving. *The British Journal of Criminology, 38*(2), 201–229. https://doi.org/10.1093/oxfordjournals.bjc.a014232

Martin, J., Cunliffe, J., & Munksgaard, R. (2019). *Cryptomarkets: A research companion*. Emerald Group Publishing.

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

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., & 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., & 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., & 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., & 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

Nelder, J. A., & Wedderburn, R. W. (1972). Generalized linear models. *Journal of the Royal Statistical Society: Series A (General), 135*(3), 370–384. https://doi.org/10.2307/2344614

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

Paquette, S., & 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., 2021*(04), 387–402.

Paternoster, R., Bachman, R., Kerrison, E., O'connell, D., & Smith, L. (2016). Desistance from crime and identity: An empirical test with survival time. *Criminal Justice and Behavior, 43*(9), 1204–1224.

Péloquin, O., Fortin, F., & Paquette, S. (2022). Examining negative online social reaction to police use of force: The George Floyd and Jacob Blake events. *Canadian Journal of Criminology and Criminal Justice, 64*(1), 53–81. https://doi.org/10.3138/cjccj.2021-0030

Penna, L., Clark, A., & Mohay, G. (2005). Challenges of automating the detection of paedophile activity on the internet. In *First international workshop on systematic approaches to digital forensic engineering (SADFE'05)*.

Piquero, A. R., & Tibbetts, S. G. (2002). *Raional choice and criminal behavior: Recent research and future challenges*. Routledge.

Reale, K. (2022). Criminal expertise and sexual violence: An examination of the crime-commission process Simon Fraser University. Burnaby, Canada https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwitwI2apdv7AhXElIkEHXiGADgQFnoECAUQAQ&url=https%3A%2F%2Fsummit.sfu.ca%2F_flysystem%2Ffedora%2F2022-08%2Finput_data%2F22317%2Fetd21873.pdf&usg=AOvVaw1ZFta7cCmPSLNS-DG_I2zV.

Reale, K., Beauregard, E., & 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., & Chopin, J. (2021b). *Expert versus novice: Criminal expertise in sexual burglary and sexual robbery sexual abuse*. https://doi.org/10.1177/10790632211024236

Reale, K., Beauregard, E., & Chopin, J. (2021c). The role of criminal expertise in serial sexual offending: A comparison to "novices". *Journal of Criminal Psychology*. https://doi.org/10.1108/JCP-07-2021-0032. Advanced Online Publication.

Rekik, R., Kallel, I., Casillas, J., & 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

Robbins, S. S., & Stylianou, A. C. (2003). Global corporate web sites: An empirical investigation of content and design. *Information & Management, 40*(3), 205–212. https://doi.org/10.1016/S0378-7206(02)00002-2

Rossmo, K. (2006). Criminal investigative failures: Avoiding the pitfalls. *FBI L. Enforcement Bull., 75*, 1.

Rossmo, K. (2009). *Criminal investigative failures*. CRC Press.

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

Steel, C. M., Newman, E., O'Rourke, S., & 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*, Article 300971. https://doi.org/10.1016/j.fsidi.2020.300971

Stefanska, E. B., & Carter, A. J. (2019). Whiter than white: The art of delaying detection in sexual killers. *International Journal of Offender Therapy and Comparative Criminology*. https://doi.org/10.1177/0306624X19840954, 0306624X19840954.

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

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

Topalli, V., Jacques, S., & Wright, R. (2015). "It takes skills to take a car": Perceptual and procedural expertise in carjacking. *Aggression and Violent Behavior, 20*, 19–25. https://doi.org/10.1016/j.avb.2014.12.001

Vicente, K. J., & Wang, J. H. (1998). An ecological theory of expertise effects in memory recall. *Psychological Review, 105*(1), 33.

Wang, Y., Guo, Y., & Chen, Y. (2016). Accurate and early prediction of user lifespan in an online video-on-demand system. In *2016 IEEE 13th international conference on signal processing (ICSP)*.

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., & 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

Yang, J., Wei, X., Ackerman, M., & Adamic, L. (2010). Activity lifespan: An analysis of user survival patterns in online knowledge sharing communities. In *Proceedings of the International AAAI Conference on Web and Social Media*.