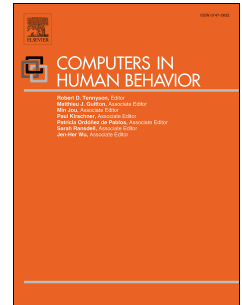


Accepted Manuscript

Lifestyles and routine activities: Do they enable different types of cyber abuse?

Zarina I. Vakhitova, Clair L. Alston-Knox, Danielle M. Reynald, Michael K. Townsley,
Julianne L. Webster



PII: S0747-5632(19)30255-9

DOI: <https://doi.org/10.1016/j.chb.2019.07.012>

Reference: CHB 6069

To appear in: *Computers in Human Behavior*

Received Date: 6 December 2018

Revised Date: 9 July 2019

Accepted Date: 14 July 2019

Please cite this article as: Vakhitova Z.I., Alston-Knox C.L., Reynald D.M., Townsley M.K. & Webster J.L., Lifestyles and routine activities: Do they enable different types of cyber abuse?, *Computers in Human Behavior* (2019), doi: <https://doi.org/10.1016/j.chb.2019.07.012>.

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

Lifestyles and routine activities: Do they enable different types of cyber abuse?

Zarina I. Vakhitova [Corresponding Author]

Monash University
Clayton Campus, Menzies Building
20 Chancellors Walk
Victoria 3800 Australia
E-mail: Zarina.Vakhitova@Monash.edu

Clair L. Alston-Knox
Griffith Social and Behavioural Research College
Griffith University
176 Messines Ridge Road, Mt Gravatt
Queensland 4122 Australia
E-mail: C.Alston-knox@Griffith.edu.au

Danielle M. Reynald
Griffith Criminology Institute
Griffith University
176 Messines Ridge Road, Mt Gravatt
Queensland 4122 Australia
E-mail: D.Reynald@Griffith.edu.au

Michael K. Townsley
Griffith Criminology Institute
Griffith University
176 Messines Ridge Road, Mt Gravatt
Queensland 4122 Australia
E-mail: M.Townsley@Griffith.edu.au

Julianne L. Webster
Griffith Criminology Institute
Griffith University
176 Messines Ridge Road, Mt Gravatt
Queensland 4122 Australia
E-mail: J.Webster@Griffith.edu.au

Lifestyles and routine activities: Do they enable different types of cyber abuse?

Abstract

Background: The emergence of new technology-facilitated types of crime following the advent of the Internet necessitated the re-examination of the utility of traditional theories such as lifestyle-routine activity theory to explain crimes that occur in the new and unique environment of cyberspace.

Reason for study: The objective of this study was to investigate whether victims' lifestyles and routine activities can help explain the risk of victimization from direct, indirect and mixed types of cyber abuse.

Research design: To achieve this objective, the data from a large nationwide (US) crowd-sourced sample ($N = 1,463$) of adult members of an online labour portal Mechanical Turk was collected using an online survey platform Qualtrics and then analyzed using Bayesian Profile Regression to identify clusters of lifestyles and routine activities of victims associated with victimization from different types of cyber abuse.

Findings: Our analyses were able to distinguish between victims and non-victims as well as between victims of different sub-classifications of cyber abuse. Specifically, we have identified five population subgroups based on their lifestyles and routine activities in terms of the associated risk of personal victimization from different types of cyber abuse. This paper discusses the differences in lifestyles and routine activities between the identified groups.

Conclusions: Our findings generally support the empirical utility of lifestyle-routine activity theory to explain cyber abuse victimization; as with other traditional types of crime (e.g. robbery or assault), victims' lifestyles and routine activities play a significant role in their risk of various types of cyber abuse victimization.

Keywords: cyber abuse, lifestyle-routine activity theory, Bayesian Profile Regression, victimization.

1 Introduction

The emergence of new types of technology-facilitated crimes compelled criminologists to re-examine the utility of traditional crime theories in the context of new environment of cyber space. Despite the major developments in this area, the question still remains: to which extent are traditional criminological theories useful for explaining new types of crime such as cyber abuse? With this question in mind, a growing body of empirical research tested the utility of traditional theories in the context of cybercrime (Holt and Bossler, 2014). Studies by Bossler et al. (2012), Hinduja and Patchin (2009), Holt et al. (2009), Holt and Bossler (2014), Leukfeldt and Yar (2016), Marcum et al. (2010), Ngo and Paternoster (2011), and Reyns et al. (2011b) and others focused on arguably the most challenging group of theories to apply to cyber crimes, namely opportunity theories such as routine activity theory (RAT) (Cohen and Felson, 1979) and lifestyle-exposure theory (LRAT) (Cohen et al., 1981). The biggest challenge in the application of these types of theories to cyberspace is in the potential conflict between the theoretical requirement for offenders and targets to converge in *time* and in *space* in order for crime to occur and the “chronically spatio-temporally disorganised” environment of cyberspace (Yar, 2005, p. 424). To date, this scholarship produced mixed results (Vakhitova et al., 2016).

The nature of the samples examined in previous research (mostly small samples of college students), the types of analytical approaches (conventional regression analyses using the Wald test that are more suitable for large samples), the way cyber abuse was operationalized in these studies (mostly as one uniform type of crime rather than distinct sub-classifications based on a theoretically derived rationale), as well as the choice of proxies to measure the key theoretical concepts in the new environment of cyberspace makes it difficult to tease out the effect of lifestyles and routine activities as risk factors across these studies (Vakhitova et al., 2016). The overarching goal of this study is therefore to evaluate the empirical utility of LRAT to explain different sub-classifications of cyber abuse victimization using robust methodology and innovative analytical approach. To achieve this objective, we analyzed a large sample ($N = 1,493$) of American adults using Bayesian Profile Regression to form clusters of similar covariate profiles that model the risk of cyber abuse. This study contributes to both theoretical and empirical literature on the utility of traditional theories of crime to explain new types of victimization. We start by reviewing the existing literature on the application of LRAT in the context of cyber abuse victimization with the focus on the operationalization of the key theoretical concepts.

2 Research testing lifestyle-routine activity theory in the context of cyber abuse victimization

Originally developed to explain criminal victimization in the physical world, LRAT integrates core ideas from two theoretical perspectives—routine activity theory (Cohen and Felson, 1979) and lifestyle exposure theory (Hindelang et al., 1978)—and focuses on the differential risk of criminal victimization as the function of differences in victims’ lifestyles and routine activities (Cohen et al., 1981). The theory encapsulates the risk within four main concepts: exposure to risk, proximity to offenders, target attractiveness, and absence of capable guardianship. The basic premise of the theory is that those who are more exposed to risk, are in closer proximity to offenders, are more attractive as targets and are not protected by capable guardians are more likely to experience victimization.

With the first two concepts rooted in spatial characteristics of the physical world—physical visibility and accessibility due to the distance between potential offenders and victims—the theory’s explanatory scope is limited, according to its creators, to only “those predatory violations involving direct physical contact between at least one offender and at least one person or object, which that offender attempts to steal or damage” (Cohen et al., 1981, p. 508). It also makes the application of the theory in the new environment of cyberspace, where space takes on a different meaning, a particular challenge.

Previous cyber abuse studies commonly operationalized exposure to risk using the amount of time spent or the number of activities performed online—for example, hours spent online and, in chat rooms, and using social networking sites, email, or instant messaging (Bossler et al., 2012; Holt et al., 2009; Marcum et al., 2010). Only a very small proportion of these proxies measuring exposure to risk were found to be significant predictors of cyber abuse victimization (Vakhitova et al., 2016). For example, in a study by Ngo and Paternoster (2011), not one proxies was found to be predictive of cyber abuse victimization, which made the authors question the value of these proxies, and suggest that simply being online may not be inherently risky. Instead, they suggested that the activities that involve active interaction with others (e.g. participation in online forums) as opposed to passive consumption of content (e.g. watching YouTube videos) may be better predictors of cyber abuse victimization. While cyber abuse studies commonly measured the combined effect of exposure to risk and proximity to offenders, a study by Reyns et al. (2011b) explicitly measured proximity to offender using proxies of adding strangers to friend list, number of friends on social network and utilizing friend service. The rationale for these proxies appears to be—offenders are strangers and, the more strangers

who have access to you, the more likely you are to experience victimization.

The third factors that contributes to the overall risk of victimization, as measured by lifestyle-routine activity theory, is target attractiveness, which represents “the material or symbolic desirability of persons or property targets to potential offenders, as well as the perceived inertia of a target against illegal treatment (i.e., the weight, size, and attached or locked features of property inhibiting its illegal removal and the physical capacity of persons to resist attack)” (Cohen et al., 1981, p. 508). In terrestrial research, target attractiveness has been measured using a number of indicators such as family income, social class, rate of unemployment, ownership of expensive and portable goods and possession of cash and precious goods such as jewellery (Miethe and Meier, 1990; Miethe and Meier, 1994; Sampson and Wooldredge, 1987).

Considering the specifics of the environment and the likely effect of offender-victim relationship on the interpretation of target attractiveness by the offender, clearly, translating this concept to the new environment of cyberspace is a challenge. The proxies used to operationalize target attractiveness in the context of cyber abuse include such diverse measures as being female, non-white, having a high academic standing and high grade point average (GPA) (Bossler et al., 2012), or relationship status and sexual orientation Reyns et al. (2011b). It is probably not a surprise proxies that resemble the measures used in terrestrial research are not particularly useful in the context of cyber abuse victimization. For example, in a more recent study, Leukfeldt and Yar (2016), none of the *material desirability* variables (e.g. personal income, household income, financial assets, financial possessions, or savings) was associated with an increased risk of cyber abuse victimization. Similarly, none of the target attractiveness variables were significant predictors of cyber abuse in Ngo and Paternoster (2011).

And finally, the concept of *capable guardianship* reflects the idea that an offender’s decision-making process is affected by the presence of a third party at the scene of a potential crime, which is seen as increasing the risk associated with the crime (Cohen and Felson, 1979; Cohen et al., 1980; Reynald, 2009; Miethe and Meier, 1994). Traditionally, guardianship has been conceptualized as having physical, personal and the presence of human third party dimensions. The corresponding measurements used in the early research included the number of household members, number of household members over the age of 12, availability of neighbours to watch over property, use of door and window locks, burglar alarms, CCTV cameras, and other similar proxies (Miethe and Meier, 1994; Reynald and Elffers, 2015).

In the context of cyberspace, operationalizations used to measure guardianship appear to have

been inspired by the terrestrial research and for most part found to be not significant predictors of victimization (Vakhitova et al., 2016). For example, van Wilsem (2013), measured the physical dimension of guardianship against cyber harassment using “computer prevention” variable, which reflected the use of computer security measures employed by the respondent, such as firewall, virus scanner, anti-spyware, Trojan scanner, spam filter, security for wireless Internet, and personal dimension by variables “low skill level” estimating the respondent’s knowledge about the security measures utilized by his or her own computer—both non-significant predictors of victimization. Similarly, a more recent study by Leukfeldt and Yar (2016) also measured multiple dimensions of guardianship: personal dimension through “computer knowledge” and “online risk awareness”, and physical dimension through “no virus scanner”.

To date, no study that we are aware of, measured the presence of a human third party as guardianship. This is important considering the latest theoretical developments in the area of capable guardianship. Building on Felson (2006), Reynald (2009) established that capable guardianship depends on someone being 1) willing to supervise, 2) able to detect potential offenders, and 3) willing to intervene when necessary. These dimensions could be summarized into two main components: availability (being in the right place at the right time, and able to detect the criminal activity) and willingness to intervene if necessary. The model of guardianship-in-action (GIA) has been examined in terrestrial research, but so far no known studies attempted to operationalize these dimensions of guardianship capability when it comes to measuring guardianship against cybercrime, in particular, cyber abuse. It is not clear whether the GIA model is useful at all in the context of cyberspace considering the unique characteristic of the environment that render potentially problematic the idea of deterrence associated with someone simply being present at the scene of a crime (as per the original formulation of routine activities theory).

As this review showed, previous research employed a variety of different proxies to measure the key lifestyles and routine activities-related theoretical concepts with most not useful for explaining the risk of cyber abuse victimization. It is possible the variables selected on the basis of the previous terrestrial literature and not specifically derived for the environment of cyberspace may not be reflective of the unique characteristics of the environment in which cybercrimes occur.

3 Current study

The review of literature highlighted the distinct lack of clarity about the utility of traditional theories of crime such as LRAT to explain new types of crime that occur in cyberspace. The goal of this

study therefore is to model victimization that occurs in cyberspace using the LRAT-related concepts to encapsulate the risk. This study focuses on one type of cybercrime—cyber abuse—defined as any behaviour that involves the use of technology to stalk and/or harass adult victims (Bocij, 2006)¹ and its specific sub-classifications—*direct* and *indirect* according to the method used to perpetrate these behaviours (Ellison and Akdeniz, 1998).

This paper contributes to the existing cyber-victimization and LRAT related literature in several ways. First, we examine the utility of LRAT in the context of a new type of crime—cyber abuse. Second, we empirically test whether different methods of cyber abuse (direct, indirect or mixed) are associated with victims’ differing lifestyles and routine activities. Finally, we extend LRAT by considering how an individual’s interpersonal relationships could serve as protective or risk factors in the context of cyber abuse victimization. This paper develops further the concept of risk in the context of cyber abuse, informing crime prevention strategies.

4 Methodology

With the objective of investigating whether specific lifestyles and routine activities are associated with varying levels of risk from different types of cyber abuse (i.e. direct, indirect and mixed), we conducted a survey of American adults—members of an online labour portal Amazon’s Mechanical Turk—and then analyzed the data using the Bayesian Profile Regression procedure².

To collect the information about the experiences of our respondents with cyber abuse victimization, an online questionnaire was designed using Qualtrics Online Platform. Questions were developed specifically for this study. The survey took no longer than 15 minutes to complete. An online survey was selected for data collection as it allows relatively easy access to a large pool of potential respondents and is cost effective. Further, compared with traditional methods of data collection, such as face-to-face or phone interviews, online surveys are associated with reduced interviewer-induced measurement errors and social desirability bias (Baker et al., 2010; Sue and Ritter, 2012; Chang and Krosnick, 2009; Kreuter et al., 2008).

In our survey, we collected the information related to one dependent variable and 31 independent variables. The modelling procedures employed involved a two-stage process whereby multiple variables measuring the same concept (e.g. proximity to offenders) were first tested using a variable selection procedure and only the most viable ones were then included in the final model.

4.1 Sampling

To identify lifestyle and routine-activities related patterns of behaviour associated with cyber abuse victimization, a large ($N = 1,463$), nationally representative sample of adults—members of Amazon’s Mechanical Turk³—was surveyed using an online questionnaire⁴.

Given that the focus of this study is on understanding cyber abuse—a crime that affects adults—we limited participation in our study to residents of the United States of America who were at least 18 years old. The workers were offered a small monetary compensation (US\$0.35) for their participation in the research (a completed survey), commensurate with the average amount of time required to complete the survey. Research suggests this approach improves response quality in Mechanical Turk surveys (Peer et al., 2013). The rate of missing data in the survey—both from break-offs and item non-response—was low. In total, 1,623 workers began the survey, and 1,463, or slightly over 90 per cent, completed the survey. Only completed surveys were included in the analyses.

4.2 Dependent variable

In this study, we follow Ellison and Akdeniz (1998) classification of cyber abuse, which groups different related behaviours according to the method used to perpetrate them as either *direct* or *indirect* cyber abuse. In this context, *direct cyber abuse* is delivered by the offender directly to the victim via abusive emails or text messages, by posting comments on the victim’s social media pages, or through covert surveillance of the victim’s activities (Vakhitova et al., 2018). In contrast, *indirect cyber abuse* is delivered with minimal or no direct interaction between the victim and the offender. Indirect cyber abuse does not require knowledge of the victim’s personal contact information. These methods of abuse include posting damaging information about the victim on a non-victim’s social media pages or web sites (Vakhitova et al., 2018). This updated classification of cyber abuse is particularly useful if we consider the potential to develop targeted crime prevention strategies. It would appear logical that behaviours that involve direct contact between offenders and victims would require a prevention approach different from the one needed to prevent behaviours that do not require direct contact.

In addition to direct and indirect categories we also consider *mixed cyber abuse* defined as the use of two or more methods of cyber abuse—at least one direct and one indirect method—employed within one incident of abuse. To be considered an instance of mixed cyber abuse, the related acts within a single incident must be motivated by the same source of conflict, occurring between the same individuals and within a limited time frame.

To analyze the difference between non-victims and victims of three types of cyber abuse—direct,

indirect and mixed—we first asked our respondents whether they had experienced any form of cyber stalking or cyber harassment directed at them personally. To ensure the respondents were clear about the types of behaviours in which we were interested, the respondents were provided with a definition of cyber abuse and a number of examples of the different forms of cyber abuse victimization.

Respondents who reported experiencing cyber abuse, were then asked to think about the most recent or most memorable incident they experienced and to select one or more specific behaviours they experienced from the list: 1) you received a text message, email or a private message via social media addressed to you personally; 2) someone posted derogatory, embarrassing information (documents, photos, videos, etc.) about you on the Internet or distributed it to others via email, text (SMS) or other technology; 3) you were subscribed to unwanted services, products, activities and you only found out about the subscription after you started to receive the services or products or were invited to participate in the activities; 4) someone, pretending to be you, sent email or text messages or private messages on social media pages to your family, friends, co-workers, or other third parties; 5) your daily activities been monitored by someone via social media or a tracking software; 6) someone created a website or a social media page containing derogatory or embarrassing information about you. Direct cyber abuse was coded for options 1 and 5, and indirect cyber abuse for options 2, 3, 4 and 6. We also coded *mixed cyber abuse* for any combination of 1 and/or 5 with any combination of 2, 3, 4, and/or 6.

By combining the information from these two questions (about the fact of victimization and the specific type of victimization), we created a four-level factor variable *Victimization* (direct = 0, indirect = 1, mixed = 2, non-victim = 3). The resulting variable had levels in the following proportions: direct ($n = 309$; 20%), indirect ($n = 168$; 11%), mixed ($n = 269$; 19%), and non-victims ($n = 717$; 50%).

4.3 Independent variables

To model cyber abuse victimization processes, we have included a number of independent variables representing various lifestyles and routine activities previously identified in Vakhitova et al. (2016). The variables were grouped to represent four key theoretical concepts: 1) exposure to risk, 2) proximity to offenders, 3) target attractiveness, and 4) capable guardianship. Table 1 presents descriptive statistics for independent variables. Please note, due to the variable selection procedure undertaken as part of the modelling process, some independent variables described here were excluded from the final model.

4.3.1 Exposure to risk

In the context of cyber abuse, we conceptualized *exposure to cyber risk* as the visibility and accessibility of the person to the potential cyber offenders provided by their online activities (see Vakhitova et al. (under review)). To measure the level of exposure to cyber risk, we asked our respondents: how often (if ever) they: 1) conduct professional activities online (e.g. as a writer, a blogger, journalist, photographer, media personality); 2) participate in online community activities or perform volunteer duties online (for example, serve as the moderator of an online forum, social media page, news or media site, online gaming site and so on); 3) use the Internet and social media to promote themselves or their causes (social, political, charitable, or others). All three variables were measured on a decimal scale from 0.0 to 2.0, where 0.0 = never and 2.0 = often/regularly. The respondents were able to pick any position on a sliding scale and the corresponding number between 0.0 and 2.0 to better reflect their estimation of the frequency.

4.3.2 Proximity to offenders

In this study, we conceptualized *proximity to cyber offenders* as being virtually (as opposed to physically) present in the domains of influence of potential cyber abusers. For example, certain sites and social media hubs (e.g. online discussion forum Reddit) have a reputation for attracting “trolls”⁵. In this study, we measure proximity to offenders by asking the participants how frequently (on a decimal scale from 0.0 to 2.0, where 0.0 = never and 2.0 = often) they: 1) participate in discussions in online forums (e.g. Reddit); 2) participate in online multi-player games; 3) post comments on social media platforms such as Facebook, YouTube, and so on.; 4) post about their personal life online; and 5) post in the comments sections of online newspapers. The respondents were able to pick any position on the sliding scale and the corresponding number between 0.0 and 2.0 to better reflect their estimation of the frequency. It should be noted that while the concepts of exposure to cyber risk and proximity to cyber offenders are not completely separate and largely overlap, the main point of difference is whether the individual performs online activities on his or her own online “turf” or whether they enter someone else’s domain. The former is reflective of exposure to cyber risk, while the latter is more reflective of proximity to cyber offenders.

4.3.3 Target attractiveness

The original physical-world definition of *target attractiveness* was conceptualized as “the material or symbolic desirability of persons or property targets to potential offenders, as well as the perceived

inertia of a target against illegal treatment (i.e. weight, size, and attached or locked features of property inhibiting its illegal removal and the physical capacity of persons to resist attack)” (Cohen et al., 1981, p. 508). In this study, we adapt this physical-world definition to the context of cyber abuse as having a symbolic value to the cyber offender, while at the same time being perceived as vulnerable to not actively or successfully resisting.

To measure the symbolic value to the cyber offender we asked our respondents whether—at the time of the incident (for victims) or now (for non-victims)—they identified as a social media personality, public figure (for example, a politician), activist, celebrity (including minor or local), or community leader (yes, no).

The vulnerability aspect of target attractiveness was measured by asking our participants about the frequency with which they participate in online discussions of topical issues (i.e. politics, the environment, gender, race, sexuality, parenting or family dynamics, religion, or spirituality). The variable is measured on a decimal scale from 0.0 to 2.0, with 0.0 = never and 2.0 = often/regularly. The respondents were able to pick any position on the sliding scale (and the corresponding number) between 0.0 and 2.0 to better reflect their estimation of the frequency.

4.3.4 Capable guardianship

Following Reynald (2010) model of guardianship in action, we measured different levels of capable guardianship intensity—witnessing and intervention—as different forms of a presence of a human third party. In this context, the former represents guardian’s availability and the skill to recognize the event as criminal, and the latter is the expression of guardian’s willingness to intervene when necessary. Specifically, to measure *witnessing*, we asked the respondents who indicated they have experienced cyber abuse whether, to the best of their knowledge, anyone has witnessed the incident of victimization. Then, to measure *intervention* we asked whether, to the best of his or her knowledge, anyone has intervened in the incident.

Following Vakhitova and Reynald (2014, p. 163), we operationalized intervention by a guardian as “any active involvement by a third party in the incident of cyber abuse by either reporting to the police, the social media site, or the Internet service provider, by contacting the offender... or by any other involvement with the goal of disrupting the cyber abuse event”. The respondents who indicated no prior cyber abuse victimization experience were asked a set of hypothetical questions: “If someone stalked or harassed you online, do you think someone would witness it?” (measuring witnessing) and “If someone stalked or harassed you on-line, do you think someone would intervene to stop it on your

behalf?” (measuring intervention).

Admittedly, these measurements of capable guardianship are not likely to be perfect. As the review of the existing cyber abuse scholarship showed, operationalization of capable guardianship, whether in cyberspace or in physical space, is a very challenging task. It is generally very difficult to measure something that did not occur—prevented victimization—the presumed effect of capable guardianship. Obviously, if guardianship worked, victimization would not have occurred. And if victimization did occur, then presumably, guardianship either was not present or did not work. To supplement these relatively direct measurements of capable guardianship, we also developed a set of proxies that measure the level of social interactions that the respondents participate in with some regularity.

Specifically, we hypothesized that those individuals with lower than average number of regular social interactions are more likely to be abused due to the reduced number of *potential guardians* in their lives. To measure the potential for guardian’s availability, we created a number of relationship-based variables, including: 1) family, 2) spouse or romantic partner, 3) ex-spouse or ex-partner, 4) acquaintances, 5) friends, 6) online gaming contacts, 7) social media contacts, 8) business or work contacts, 9) sport, social club or committee contacts, and 10) education contacts. We grouped these social connections according to the perceived centrality of these relationships in one’s life into: 1) primary relationships, 2) peripheral relationships, and 3) online relationships (see Table 1). We expect that the presence of potential guardians will decrease the likelihood of victimization, while other lifestyle and routine activity related variables will increase it.

4.4 Demographic controls

The latest research in cyber abuse victimization provides evidence to support the inclusion of demographic variables as controls in the overall model. For example, according to the Internet safety group *Working to Halt Online Abuse*, the majority (87%) of cyber abuse victims are female. A study by the Pew Research Center has shown age, gender and race/ethnicity are the factors for cyber abuse victimization, with younger people, males and blacks being disproportionately more likely to experience online harassment (Duggan, 2017).

To account for the potential effect of demographic characteristics on the risk of personal victimization from cyber abuse suggested in previous research (Hindelang et al., 1978; Reyns et al., 2011a), the analysis included: *age* (in years), *gender* (female = 1), *race/ethnicity* (white = 1), and *employment status* (employed = 1). To measure the demographic characteristics of the respondents at the time

of the cyber abuse incident, we asked our respondents (victims) to provide us with information that reflected that time—for example, “Around the time of the incident, what was your age?”. To measure race/ethnicity, we listed a number of categories including white/Caucasian; black, African American; American Indian or Alaska native; Hispanic, Latino, or Spanish origin; Asian (Chinese, Asian Indian, Filipino, Japanese, Korean, Vietnamese, etc.); Pacific Islander (Native Hawaiian, Guamanian, or Chamorro, Samoan, etc.); mixed; other. At the data coding stage, we created a new binary variable “race” where all categories other than white/Caucasian were coded as 0 and white as 1. Likewise, to measure employment, we listed several categories, including: employed full-time; employed part-time; self-employed; student (not employed); homemaker (not employed); unemployed; and other. We then created a new binary variable with two possible values, where 1 = employed including those employed full-time, employed part-time and self-employed, and 0 = unemployed, including all other categories.

4.5 Analytic strategy

A standard regression approach to this survey would usually involve a generalized linear model for multinomial data (Agresti, 2013). However, as evidenced by a number of studies (see, e.g. Patterson et al. (2002) and Molitor et al. (2010)), social surveys often produce a set of highly inter-related variables. A correlation matrix for *target attractiveness (vulnerability)* variables related to discussing contentious issues online (shown in Figure 1) suggests that many of these variables in our study are highly correlated, and this will make their inclusion in a standard regression model problematic.

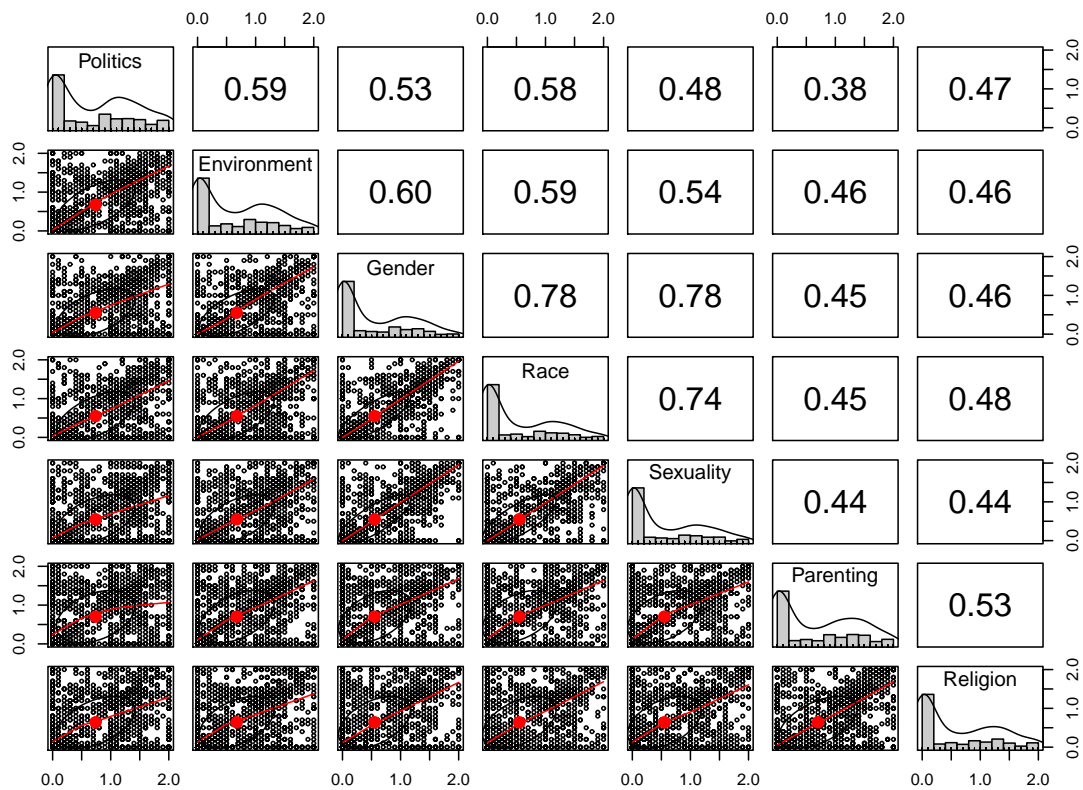


Figure 1: Correlation matrix for target attractiveness (vulnerability) variables

Molitor et al. (2010) suggest that, as standard regression analyses often have issues when exploring beyond main effects due to surveys producing a large number of covariates—which, by the nature of the research, should be inter-related—profiling (clustering) is likely to produce a more intuitive outcome. This will enable better exploration of the key indicators that can be derived from the survey.

Figure 2 illustrates, in more detail, the correlation of two variables (online discussion of *environmental issues* and *politics*) from Figure 1. Observing the scatter plot, in the green ellipse, we see a cluster of respondents who make a similar amount of posts online on both topics, and these responses contribute to the reasonably large correlation (0.59). However, moving beyond the main effects of each variable, we note the blue ellipses, which indicate respondents who may post on one variable, but not the other, and between these ellipses, we have many other levels of response relationships.

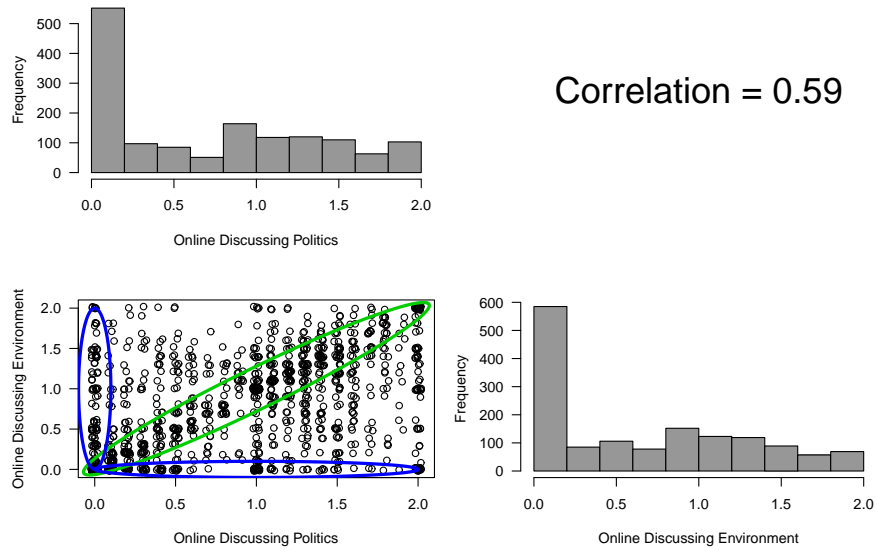


Figure 2: Correlation and pairwise plots for target attractiveness (vulnerability) variables related to online discussions of *environmental issues* and *politics*

As noted in Vakhitova and Alston-Knox (2018), in terms of a logistic regression, modelling interactions in a generalized linear model is complicated by the implicit interaction resulting in the back-transformation of a main effects model to the natural scale (Tsai and Gill, 2013), and the additional interaction that may be added to the model. For this reason, we are analyzing the data using the Bayesian Profile Regression analysis, as described below.

4.5.1 Bayesian Profile Regression with variable selection

Bayesian Profile Regression (BPR) is a recently developed technique that allows modelling when multiple highly correlated covariates are present by partitioning the subjects into groups according to covariate profile (Papathomas et al., 2012; Molitor et al., 2010). BPR appears to be superior to earlier clustering methods such as latent class analysis and cluster analysis, as “it allows the number of groups to vary, uncovers subgroups and examines their association with an outcome of interest, and fits the model as a unit, allowing an individual’s outcome potentially to influence cluster membership” (Molitor et al., 2010, p. 484). An original impetus for the technique can be found in Molitor et al. (2010), who analyzed a national telephone survey in the United Kingdom as part of a child and adolescent health initiative. Hastie et al. (2013) provides an example analysis of lung cancer and its relationship with smoking. A comparison of standard logistic regression and BPR using a case

study related to lung cancer and its relationship with solvent exposure can be found in Mattei et al. (2016), and an example from dementia studies can be found in El-Saifi et al. (2018). While to date, BPR has been used mainly in health and medical research, it has a very wide potential scope of application, including in social sciences such as criminology. For a detailed description of Bayesian Profile Regression please see Appendix A.

Taking into account the risk of over-fitting and lack of precision, associated with including a large number of variables (31) in the explanatory model, prior to BPR, we conducted a variable selection analysis using statistical procedures in the PReMiuM package (Papathomas et al., 2012). By so doing, we ensured that our explanatory model is parsimonious and that only the variables that contribute to the overall effect are included in the model (McQuarrie and Tsai, 1998; Burnham and Anderson, 2002).

In cases where we measured multiple variables that tended to be associated with the same theoretical concept, we used the binary cluster variable selection algorithm in the PReMiuM package to determine which variable most actively described the clusters of the respondents (Papathomas et al., 2012; Liverani et al., 2015). When the subjects' profiles are formed by many covariates, it is often the case that a considerable number do not contribute to the clustering. This variable selection procedure, which resulted in selecting 22 of the initial 31 variables, allowed us to identify the covariates that are most informative in the formation of clusters. For a detailed description of the variable selection procedure please see Appendix B.

5 Results

Table 1 presents the descriptive statistics for the sample. The final sample is very similar to the general US population with a median age of 47.4, compared with 34.9 in our sample, 47.9 per cent male, compared with 48 per cent in our sample and 70.5 percent white compared with 73.0 percent in our sample (*U.S. Census Bureau Quick Facts* 2018).

Table 1 Descriptive characteristics of the sample ($N = 1,463$)

Variables	Mean	SD	Min	Max
Demographic controls				
(1) Age	34.90	12.60	13**	80
(2) Gender (female)	0.52	0.50	0	1
(3) Race (white)	0.73	0.44	0	1
(4) Employment (employed)	0.80	0.40	0	1
Independent variables				

Continued on next page

Table 1 – Continued from previous page

Variables	Mean	SD*	Min	Max
<i>Exposure to risk</i>				
(5) Professional/semi-professional activities	0.65	0.70	0	2
(6) Volunteer online	0.48	0.63	0	2
(7) Use the Internet to promote oneself	0.78	0.68	0	2
<i>Proximity to offenders</i>				
(8) Participate in discussions in online forums	0.91	0.66	0	2
(9) Participate in online multi-player gaming	0.72	0.73	0	2
(10) Posting about your personal life online	0.93	0.64	0	2
(11) Posting in the comments sections of online newspapers and social media	1.12	0.65	0	2
<i>Target attractiveness</i>				
Vulnerability: Discussing topical issues online				
(12) Politics	0.74	0.68	0	2
(13) Environment	0.67	0.64	0	2
(14) Gender	0.55	0.62	0	2
(15) Race	0.55	0.63	0	2
(16) Sexuality	0.55	0.63	0	2
(17) Parenting	0.70	0.68	0	2
(18) Religion	0.64	0.67	0	2
(19) Symbolic value: Celebrity/public figure	0.11	0.31	0	2
<i>Guardianship</i>				
(20) Guardianship: Witnessing cyber abuse	1.07	0.83	0	2
(21) Guardianship: Intervention in cyber abuse	0.90	0.86	0	2
<i>Guardianship through social interactions</i>				
<i>Guardianship: Primary relationships</i>				
(22) Family ($n = 1,095$)	0.75	0.44	0	1
(23) Friends ($n = 1,076$)	0.73	0.50	0	1
(24) Spouse, romantic partner ($n = 749$)	0.51	0.50	0	1
<i>Guardianship: Online relationships</i>				
(25) Online gaming connections ($n = 200$)	0.14	0.34	0	1
(26) Social media connections ($n = 743$)	0.51	0.50	0	1
<i>Guardianship: Peripheral relationships</i>				
(27) Acquaintances ($n = 695$)	0.47	0.49	0	1
(28) Sports and social committee connections ($n = 212$)	0.14	0.34	0	1
(29) Education connections ($n = 304$)	0.21	0.40	0	1
(30) Business, work connections ($n = 640$)	0.44	0.40	0	1
(31) Ex-spouse, romantic ex-partner ($n = 180$)	0.12	0.33	0	1

*Abbreviations: SD—standard deviations

**Age at the time of the incident.

All respondents were at least 18 years of age at the time of the survey.

5.1 Risk profiles identified by Bayesian Profile Regression (BPR)

BPR produced a representative clustering dividing our sample into five clusters (profiles)⁶. All five clusters were of a similar membership size: Profile 1 ($n = 283$), Profile 2 ($n = 347$), Profile 3 ($n = 313$), Profile 4 ($n = 261$), and Profile 5 ($n = 259$). Each of the clusters was characterized by exposure to a specific type of cyber abuse, and non-exposure, summarized in Table 2.

Figure 3 (a, b, c and d) shows plots of clusters of cases (respondents) according to the associated risk of a) direct abuse, b) indirect abuse, c) mixed abuse, and d) non-victimization. Here, red colour indicates the mean of the profile is above average for the sample, blue is below average, and gray is about average for the sample.

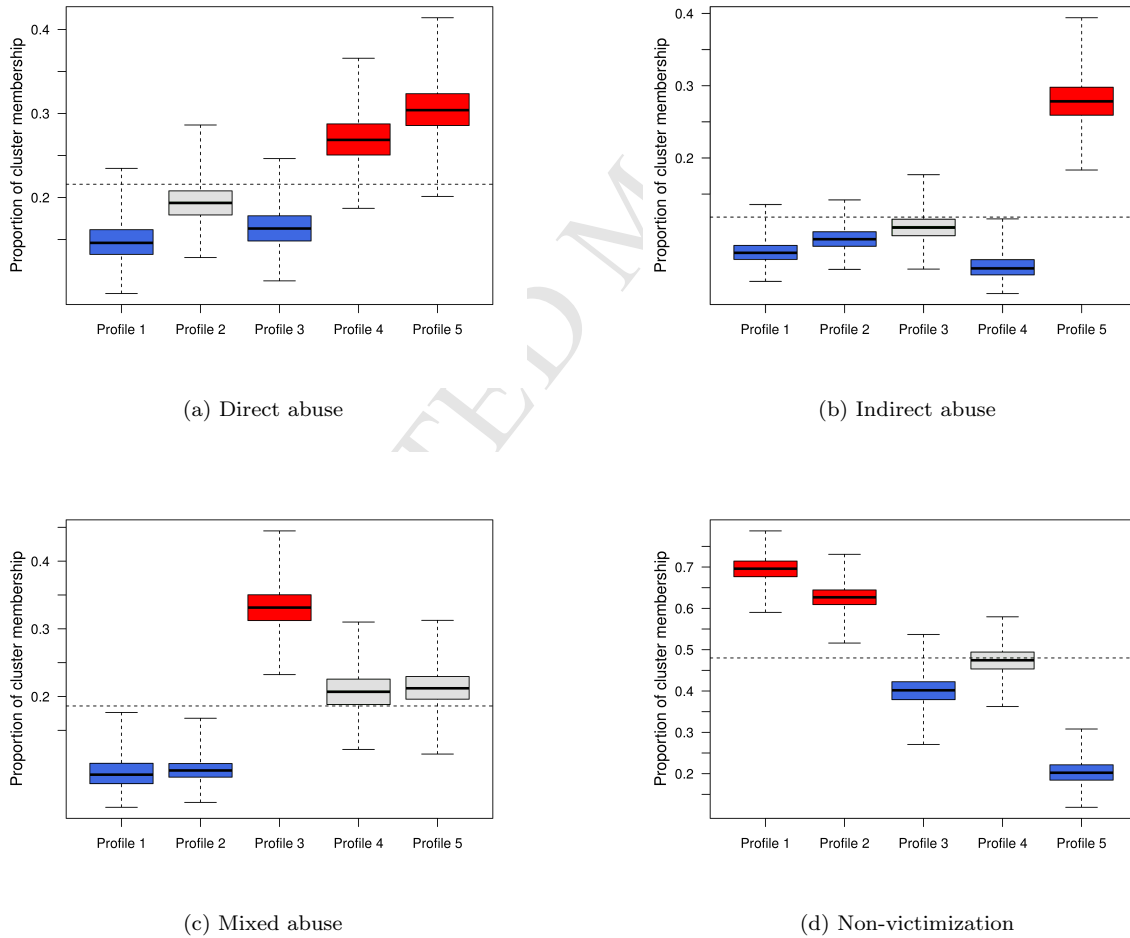


Figure 3: Risk profiles identified by Bayesian Profile Regression

Individuals fitting Profiles 4 and 5 are the most likely to experience direct methods of cyber

abuse, while those fitting Profiles 1 and 3 are the least likely. Those in Profile 5 are much more likely to experience indirect abuse compared with all other profiles. Mixed abuse is most likely to be experienced by individuals fitting Profile 3, who are unlikely to experience direct abuse and have average level of risk of experiencing indirect abuse.

Figure 3 clearly shows that individuals in Profiles 1 and 2 are most likely to be non-victims, as they are less likely to experience any type of cyber abuse compared with those in the other profiles, and individuals in Profiles 3 and 5 are the least likely of all five profiles to be non-victims. However, the probability of non-victimization for Profile 4 is less clear.

5.2 Summaries of individual profiles

Table 2 summarizes each individual risk profile. Here, red numbers signify that the mean for this profile is above average for the sample, blue numbers represent means that are below average for the sample and gray numbers represent means that are about average for the sample. For example, Profile 1 individuals have above average probability among the sample of being non-victims, meaning this group is over-represented by non-victims ($p = 0.70$), and below average probability of being victims of mixed ($p = 0.09$), indirect ($p = 0.07$) or direct ($p = 0.15$) cyber abuse, meaning that Profile 1 is under-represented by victims of any kind of cyber abuse.

Table 2: Summary of profiles

	Profiles					
	1	2	3	4	5	
Risk						
Non-victims		0.70	0.63	0.40	0.47	0.20
Mixed		0.09	0.09	0.33	0.21	0.21
Indirect		0.07	0.09	0.10	0.05	0.28
Direct		0.15	0.19	0.16	0.27	0.30
Variable						
<i>Demographics</i>						
(1) Age (standardized)		0.51	0.22	-0.13	-0.10	-0.59
(2) Gender		0.69	0.64	0.57	0.53	0.34
(3) Race		0.84	0.77	0.71	0.72	0.62
(4) Employment		0.81	0.68	0.79	0.73	0.89
<i>Exposure to risk</i>						
(5) Professional activities		0.68	0.34	0.79	0.34	1.17
(6) Volunteering		0.15	0.02	1.08	0.12	1.09
(7) Self-promotion		0.88	0.07	1.15	0.79	1.16
<i>Proximity to offenders</i>						
(8) Online games		0.16	0.43	1.01	0.94	1.12
<i>Target attractiveness</i>						

Continued on next page

Table 2 – Continued from previous page

	Profiles				
	1	2	3	4	5
(9) Discuss politics	0.83	0.06	0.91	0.95	1.13
(10) Discuss environment	0.79	0.05	0.88	0.70	1.11
(11) Celebrity	0.07	0.02	0.14	0.06	0.29
<i>Guardianship: GIA</i>					
(12) Witnessing	0.66	0.48	0.60	0.58	0.21
(13) Intervention	0.59	0.39	0.39	0.36	0.14
<i>Guardianship: Socialization</i>					
<i>Primary relationships</i>					
(14) Family	0.90	0.84	0.77	0.79	0.38
(15) Friends	0.88	0.78	0.81	0.81	0.36
(16) Spouse, romantic partner	0.66	0.55	0.53	0.55	0.24
<i>Secondary relationships</i>					
(17) Online games	0.03	0.07	0.26	0.19	0.14
(18) Social media	0.63	0.41	0.66	0.58	0.25
<i>Peripheral relationships</i>					
(19) Acquaintances	0.58	0.50	0.58	0.50	0.17
(20) Education	0.24	0.20	0.30	0.20	0.10
(21) Business	0.58	0.44	0.48	0.46	0.20
(22) Ex-spouse	0.11	0.13	0.17	0.11	0.10
Red—mean is above average for the sample, blue is below average, gray is about average.					
Red and blue numbers indicate sample average is not included in 95% credible interval					
Gray indicates sample average is contained in 95% credible interval					

5.2.1 Profile 1: Mostly non-victims, highly active, highly social

Profile 1 is characterized by over-representation of non-victims compared with what would be expected from a random sample (see Table 2). In terms of routine activities, individuals fitting this profile tend to use the Internet for self-promotion (exposure to risk) more often than expected based on the sample. These people are not likely to perform volunteer duties online. They also report below average participation in online gaming and are unlikely to socialize with other online gamers. At the same time, Profile 1 individuals get involved in discussions of the environment and politics more frequently than average. Profile 1 individuals are not likely to classify themselves as “celebrities”. Profile 1 individuals report levels of guardianship against cyber abuse (witnessing and intervention) that are relatively high. This appears to be related to the very active relational structure reported by these individuals. Profile 1 individuals are the most social of all five profiles: they have regular interactions with people from different relational groups including primary, peripheral and online—family, spouses, friends, acquaintances and business contacts. Individuals in this profile are more likely to be older, white, and female than expected based on the overall sample characteristics.

5.2.2 Profile 2: Mostly non-victims, not active, not social

Profile 2 is similar to Profile 1 in terms of the risk associated with different lifestyles, as non-victims are over-represented, with one difference being the risk of direct abuse is slightly higher than in Profile 1 and is about average for other types of abuse (see Table 2). This risk profile is associated with below average participation in online activities across the board. Profile 2 individuals also report below average passion for controversial topics—both politics and the environment. In terms of guardianship, Profile 2 individuals report average likelihood of witnessing or intervening in the event of abuse. Profile 2 individuals report above average interactions only with family and friends and below average with all online contacts. This is not surprising, as they do not appear to do much online, and therefore have little interaction with online contacts. This groups also does not contain many “celebrities”. Demographically, Profile 2 individuals are likely to be older, female and unemployed.

5.2.3 Profile 3: Mostly victims (mixed abuse), highly active, highly social

Profile 3 represents mostly victims of mixed abuse (Table 2). Profile 3 individuals appear to be very active online across the board, including in online gaming, as well as having above average involvement in discussions about politics and the environment. Profile 3 individuals register above average reports that someone will witness them being abused, but average reports that someone will intervene to stop it. These individuals have a complex relational structure: they have above average interactions with online contacts (including other gamers), marginal interactions with contacts such as acquaintances and education contacts and, surprisingly, ex-spouses. In this profile, celebrities are over-represented. In terms of their demographic characteristics, Profile 3 individuals tend to be younger, and are equally likely to be male as female, white as non-white and employed as unemployed.

5.2.4 Profile 4: Mostly victims (direct abuse), not active, somewhat social

Profile 4 is characterized by uncertain risk of victimization (Table 2). These individuals are about as likely to be victims as non-victims. If they do experience victimization, it is most likely to be of a direct kind. Like those in Profile 3, these individuals report an above average likelihood of someone witnessing the abuse, but only an average likelihood of someone intervening. Like those in Profile 3, individuals in Profile 4 report above average interaction with online contacts, but, unlike those in Profile 3, they interact with their families above the average. Further, their interaction with marginal contacts is at an average level. Demographically, Profile 4 individuals are very similar to Profile 3 individuals: they tend to be younger, but as likely to be female as male, employed as unemployed and

white as non-white, and are unlikely to be celebrities.

5.2.5 Profile 5: Mostly victims (direct or indirect abuse), highly active, not social

Victims of direct or indirect cyber abuse are over-represented in Profile 5 by a greater margin than any other profile (Table 2). Profile 5 individuals have above average involvement for the sample in various online activities, but are below average in regular social interaction with almost all types of relations, with only two exceptions—online gaming contacts and ex-spouses. Probably not surprisingly, Profile 5 individuals report below average likelihood of someone witnessing or intervening in the event of them being cyber abused. From the demographic point of view, individuals in this profile are more likely to be younger, non-white, employed, and male.

5.3 The empirical utility of lifestyle-routine activities theory to explain cyber abuse victimization

Table 2 shows that different key LRAT concepts, at least as they are represented by the chosen proxies in this study, are characterized by the varying degrees of utility to explain variations in the risk of victimization from cyber abuse and its sub-classifications. Specifically, overall, non-victims tend to report less involvement in online activities increasing their exposure to risk (in this study, measured through professional activities, volunteering and self-promotion online), however, this trend is not uniform, and the level of involvement differs according to the clustering profile.

Specifically, victims (Profiles 3 and 5) reported above average involvement in all three of these activities, while Profile 4 individuals (average risk of victimization) reported below average involvement in online professional and volunteer activities, but about average involvement in online self-promotion, and Profile 1 individuals (non-victims) reported average levels of involvement in online professional activities and above average levels of online self-promotion. It appears that, by itself, self-promotion online is not particularly useful in distinguishing victims from non-victims; however, we note that while it is above average, when present in profiles of non-victims, self-promotion is at the lower level of the range (.88 in Profile 1, compared with 1.15 in Profile 3 and 1.16 in Profile 5).

Further, in terms of activities increasing victims' proximity to offenders, non-victims appear to be less likely than victims to report participating in online gaming. However, profiles of non-victims (Profiles 1 and 2) and victims (Profiles 3 and 5) have different levels of involvement in online gaming. Among victims, those in Profile 5 are much more likely to be involved in online gaming than those in Profile 3. At the same time Profile 3 individuals (victims) and Profile 4 individuals (average risk

of victimization) demonstrate a nearly identical level of involvement in online gaming, meaning that online gaming alone does not predict whether or not the individual will become a victim of cyber abuse.

As to the measures of target attractiveness, profiles of non-victims (Profiles 1 and 2), tend to have lower proportions of “celebrities” (as operationalized in this study), while profiles of victims (Profiles 3 and 5), higher proportions. Profile 5, which is associated with the highest relative risk of victimization from direct or indirect cyber abuse, has the highest proportion of “celebrities”. Here, it is important to mention that the number of individuals who reported being a “celebrity” in our sample is, unsurprisingly, quite small ($n = 159$; 9.8%), so caution must be exercised in any conclusions about this variable.

Table 2 suggests that another aspect of target attractiveness—the victim’s vulnerability—measured through expressing one’s opinions about politics or the environment in cyberspace may be associated with a higher risk of cyber abuse victimization. Profile 2 (non-victims) are clearly not involved in discussions of politics or the environmental issues, while those in Profile 1 are much more involved and are similar in this regard to the profile of victims (Profile 3) and those average risk of victimization (Profile 4), but much less involved than those in Profile 5 (victims).

In terms of capable guardianship, there are clear differences between the profiles of victims and those of non-victims. Those in Profile 5 (victims), the loneliest of all profiles, report having guardians against cyber abuse in their lives considerably below average in comparison with not only non-victims, but also other victims (Profile 3) and those with average risk of victimization (Profile 4). Those in Profile 5 are also characterized by the highest risk of victimization from cyber abuse.

When the capable guardianship was measured the level of social interactions, the results appear to be mixed. Individuals in Profile 1 (the lowest overall risk of victimization) are the most social, while those in Profile 5 (the highest overall risk of victimization) are the least social of all profiles (see Table 2). In general, victim profiles (Profiles 3 and 5) tend to be less social than non-victim profiles (Profiles 1 and 2)). Individuals in Profiles 1 and 2 are quite social, with those in Profile 1 more social than those in Profile 2 in all types of relationships except with ex-spouses and social media⁷. Overall, it appears that having an active social life might be a protective factor for cyber abuse.

6 Discussion

To date, the opportunity theories such as routine activity theory, lifestyle exposure theory and the integrated LRAT have been successfully employed to explain a multitude of crime problems that occur

in terrestrial environment, e.g. burglary or assault. The recent scholarship testing these theories in the new environment of cyberspace produced inconsistent results making it difficult to judge the empirical utility of these theories to explain new technology-facilitated types of crimes. The main objective of this study was to ascertain the empirical utility of LRAT adapted through the use of proxies recently developed specifically for the context of cyber abuse victimization to explain different sub-classifications of cyber abuse, i.e. direct, indirect and mixed cyber abuse. To achieve this objective, this study employed an innovative method of data analysis—Bayesian Profile Regression—to examine a large non-probability data sample ($N = 1,463$) collected through an online survey of American adults.

Our findings generally support the empirical utility of LRAT to explain cyber abuse victimization as our explanatory model was able to distinguish between victims and non-victims. On average, non-victims compared with victims were found to report below average involvement in risky activities as measured in this study. In general, above average involvement in activities that increase one's exposure to risk, proximity to offenders and target attractiveness (as measured in this study) were associated with Profiles that contained mostly victims (i.e. Profiles 3-5). Conversely, below average participation was associated with Profiles that contained mostly non-victims (Profiles 1-2).

However, while being able to identify profiles of behaviours associated with victimization and non-victimization, the BPR suggests some variations in the utility of specific LRAT concepts to explain cyber abuse victimization. For example, profile of victims consistently score higher than average on proximity to offenders, measured in this study as participation in online gaming, while other concepts, such as exposure to risk, target attractiveness are less consistent in this regard (as measured in this study). It is possible that different concepts have a varying degree of explanatory power, but more likely this result could be explained by the varying degree of explanatory power of the chosen proxies.

Further, our findings suggest a level of complexity of the relationships between the key theoretical concepts not obvious from the original formulation of LRAT or previous research. In contrast to the conventional “main effects only” models commonly employed in previous studies, the BPR, revealed, that there are variations within the groups of profiles of victims and non-victims. For example, while Profile 2 is clearly lower on participation in all risky activities compared to all other profiles and it is not surprising that it contains mostly non-victims (63%), things are less obvious with Profile 1, which contains even higher proportion of non-victims (70%), but similar to profiles that contain mostly victims (Profiles 3 and 5) in terms of self-promotion, participation in discussing politics and the environment. However, Profile 1 is very low on participation in online gaming, a factor that is

distinctly associated with victims (all three victim profiles: Profiles 3 -5). Similarly, exposure to risk and target attractiveness concepts, as measured in this study, are above average only for 2 out of 3 profiles that contain mostly victims (Profiles 3 and 5). This suggests that when interaction effects are considered within the model, some explanatory effects are more useful than others.

7 Limitations

While this study contributes a number of findings to the existing knowledge base, these findings should be interpreted in the light of the limitations of this study. First, victims surveys only allow examination of the events from the victim's point of view and, like all self-report data, surveys produce data that is potentially biased (e.g. social desirability bias, recall problems, etc.). In future research, it might be beneficial to triangulate by including the data from multiple sources, including interviews or surveys of cyber abuse offenders. Second, the sample, while sufficiently large for meaningful statistical analyses, is a convenience sample and therefore can be characterized by the usual issues of non-probability samples, mainly not allowing us to make inferences about the target population (i.e. the general population of the US). Considering the goal of the analyses was not to make inferences about general population in terms of proportions or trends but instead to test the theory by modelling victimization events, this was deemed acceptable. Future research should test the findings using large probability-based samples. Third, the design of this study does not allow to identify whether the identified complex interactive relationships between the concepts are the artifact of the proxies chosen to represent the concepts or they reflect the true complex nature of the phenomenon. It is also possible, that these complex relationships are characteristic of the specific type of crime examined in this study (cyber abuse), and that the nature of the relationship between the key LRAT concepts may be different in the context of other types of crimes, especially, those occurring in different environments. More research examining the interactive nature of the relationship between the key LRAT concepts as opposed to the conventional "main effects models" approach is needed for a more conclusive set of results.

8 Conclusion

In conclusion, the overarching goal of this study was to establish the empirical utility of lifestyle-routine activity theory to explain victimization from new technological types of crimes like cyber abuse. Using an updated classification of cyber abuse, more ecologically valid measures of the key theoretical concepts, an improved methodology and the innovative analytical technique, the model

used in this study was able to distinguish between non-victims and victims of different types of cyber abuse victimization.

Our findings suggest that when carefully adapted to the specific environment—cyberspace—and the particular type of crime—cyber abuse—lifestyle-routine activity theory has a considerable empirical utility to help explain and understand crimes that occur in environments that are very different from the ones for which the theory was originally developed. By extension, this means that through careful operationalization of the key theoretical concepts, terrestrial theories such as lifestyle routine activity theory and routine activity theory could be adapted and extended to explain new and emerging types of criminality such as those that occur in the new environment of cyberspace.

Besides being able to distinguish between victims and non-victims, our analyses identified the differences in lifestyles and routine activities between victims of different sub-classifications of cyber abuse—direct, indirect and mixed. These findings indicate that sub-classifications of cyber abuse can be characterized by different patterns of lifestyles and routine activities, and therefore support the need to consider and model the processes of victimization from different sub-classifications of cyber abuse separately. Further, the unique nature of sub-classifications of cyber abuse suggests the need to develop crime prevention strategies specific for mechanisms of victimization typical of each type with lifestyles and routine activities identified as predictors of victimization treated as risk factors as targeted in developing crime prevention strategies. Overall, the results of this paper suggest that LRAT can provide useful insights into the nature of cyber abuse victimization and its causal mechanisms.

References

- Agresti, A. (2013). *Categorical data analysis*. John Wiley & Sons.
- Ansolabehere, S. & Schaffner, B. F. (2014). Does survey mode still matter? findings from a 2010 multi-mode comparison. *Political Analysis*, 22, 285–303.
- Baker, R., Blumberg, S. J., Brick, J. M., Couper, M. P., Courtright, M., Dennis, J. M., . . . Lavrakas, P. J. (2010). Research synthesis: AAPOR report on online panels. *Public Opinion Quarterly*, 74, 711–781.
- Bocij, P. (2006). *Cyberstalking: harassment in the internet age and how to protect your family*. Westpoint, CT: Praeger Publishers.
- Bossler, A. M., Holt, T. J., & May, D. C. (2012). Predicting online harassment victimization among juvenile population. *Youth Society*, 44, 500–523.

- Brickman-Bhutta, C. (2012). Not by the book: facebook as a sampling frame. *Sociological Methods & Research*, 41, 57–88.
- Burnham, K. P. & Anderson, D. R. (2002). Multimodel inference: understanding aic and bic in model selection. *Sociological Methods & Research*, 33, 261–304.
- Chang, L. C. & Krosnick, J. A. (2009). National surveys via rdd telephone interviewing versus the internet: comparing sample representativeness and response quality. *Public Opinion Quarterly*, 73, 641–678.
- Cohen, L. E. & Felson, M. (1979). Social change and crime rate trends: a routine activity approach. *American Sociological Review*, (44), 588–608.
- Cohen, L. E., Felson, M., & Land, K. C. (1980). Property crime rates in the united states: a macro-dynamic analysis. *American Journal of Sociology*, 86, 90–117.
- Cohen, L. E., Kluegel, J. R., & Land, K. C. (1981). Social inequality and predatory victimisation: an exposition and test of a formal theory. *American Sociological Review*, 46, 505–524.
- Dowling, C. M. & Wichowsky, A. (2014). Attacks without consequence? candidates, parties, groups, and the changing face of negative advertising. *American Journal of Political Science*, 59, 19–36.
- Duggan, M. (2017). Online harassment. Retrieved September 30, 2017, from <http://www.pewinternet.org/2017/07/11/online-harassment-2017/>
- El-Saifi, N., Moyle, W., Jones, C., & Alston-Knox, C. (2018). Determinants of medication adherence in older people with dementia from the caregivers' perspective. *International Psychogeriatrics*.
- Ellison, L. & Akdeniz, Y. (1998). Cyber-stalking: the regulation of harassment on the internet (special edition: crime, criminal justice and the internet). *Criminal Law Review*, 2948. Retrieved from <http://www.cyber-rights.org/documents/stalking>
- Felson, M. (2006). *Crime and nature*. Thousand Oaks, CA: Sage.
- Groenendyk, E. (2016). The anxious and ambivalent partisan: the effect of incidental anxiety on partisan motivated recall and ambivalence. *Public Opinion Quarterly*, 80, 460–479.
- Hastie, D. I., Liverani, S., Azizi, L., Richardson, S., & Stücker, I. (2013). A semi-parametric approach to estimate risk functions associated with multi-dimensional exposure profiles: application to smoking and lung cancer. *BMC Medical Research Methodology*, 13, 129:142.
- Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of personal crime: an empirical foundation for a theory of personal victimization*. Cambridge, MA: Ballinger.
- Hinduja, S. & Patchin, J. W. (2009). *Victims of personal crime: an empirical foundation for a theory of personal victimization*. New York: Corwin Press.

- Hitlin, P. (2016). Research in the crowdsourcing age, a case study. how scholars, companies and workers are using mechanical turk, a 'gig economy' platform, for tasks computers can't handle. Retrieved from <http://www.pewinternet.org/2016/07/11/research-in-the-crowdsourcing-age-a-case-study/>
- Holt, T. J. & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behaviour*, 35, 20–40.
- Holt, T. J., Blevins, K. R., & Kuhns, J. B. (2009). Exploring strategies for qualitative criminological and criminal justice inquiry using on-line data. *Crime and Delinquency*, 60, 261–283.
- Kreuter, F., Presser, S., & Tourangeau, R. (2008). Social desirability bias in cati, ivr, and web surveys: the effects of mode and question sensitivity. *Public Opinion Quarterly*, 72, 847–865.
- Leukfeldt, E. R. & Yar, M. (2016). Applying routine activity theory to cybercrime: a theoretical and empirical analysis. *Deviant Behaviour*, 37(3), 263–280.
- Liverani, S., Hastie, D. I., Papathomas, M., Richardson, S., & Azizi, L. (2015). *PReMiuM: An R package for Profile Regression Mixture Models using Dirichlet Processes*. Retrieved from <http://cran.r-project.org/web/packages/PReMiuM>
- Marcum, C. D., Rickets, M. L., & Higgins, G. E. (2010). Assessing sex differences of online victimization: an examination of adolescent online behaviours using routine activity theory. *Criminal Justice Review*, 35, 412–437.
- Mattei, F., Liverani, S., Guida, F., Matrat, M., Cenée, S., Azizi, L., ... Stucker, I. (2016). Multidimensional analysis of the effect of occupational exposure to organic solvents on lung cancer risk: the icare study. *Occupational and Environmental Medicine*. doi:10.1136/oemed-2015-103177. eprint: <http://oem.bmj.com/content/early/2016/02/23/oemed-2015-103177.full.pdf>
- McQuarrie, A. D. R. & Tsai, C. L. (1998). *Regression and time series model selection*. New Jersey: World Scientific.
- Miethe, F. D. & Meier, R. F. (1990). Opportunity, choice and criminal victimization rates: a theory of a theoretical model. *Journal of Research in Crime and Delinquency*, 27, 243–266.
- Miethe, T. D. & Meier, R. F. (1994). *Crime and its social context: toward an integrated theory of offenders, victims, and situations*. Albany: State University of New York Press.
- Molitor, J. T., Papathomas, M., Jerrett, M., & Richardson, S. (2010). Bayesian profile regression with an application to the national survey of children's health. *Biostatistics*, 11, 484–498.
- Mullinix, K., Leeper, T. J., Druckman, J. N., & Freese, J. (2015). The generalizability of survey experiments. *Journal of Experimental Political Science*, 2, 109–138.

- Ngo, F. T. & Paternoster, R. (2011). Cybercrime victimization: an examination of individual and situational level factors. *International Journal of Cyber Criminology*, 3, 773–793.
- Papathomas, M., Molitor, J., Hoggart, J., Hastie, D., & Richardson, S. (2012). Exploring data from genetic association studies using bayesian variable selection and the dirichlet process: application to searching for gene-gene patterns. *Genetic Epidemiology*, 36, 663–674.
- Pasek, J. (2016). When will nonprobability surveys mirror probability surveys? considering types of inference and weighting strategies as criteria for correspondence. *International Journal of Public Opinion Research*, 28, 269–291.
- Patterson, B. H., Dayton, C. M., & Graubard, B. I. (2002). Latent class analysis of complex sample survey data: application to dietary data. *Journal of the American Statistical Association*, 97, 721–728.
- Peer, E., Vosgerau, J., & Acquisti, A. (2013). Reputation as a sufficient condition for data quality on amazon mechanical turk. *Behavior Research Methods*, 46, 1023–1031.
- Pickett, J. T. & Bushway, S. D. (2015). Dispositional sources of sanction perceptions: emotionality, cognitive style, intolerance of ambiguity, and self-efficacy. *Law and Human Behavior*, 39(6), 624–640.
- Pickett, J. T. & Roche, S. P. (2017). Questionable, objectionable or criminal? public opinion on data fraud and selective reporting in science. *Science and Engineering Ethics*. doi:10.1007/s11948-017-9886-2
- Pickett, J. T., Roche, S. P., & Pogarsky, G. (2018). Toward a bifurcated theory of emotional deterrence. *Criminology*, 56(1), 27–58.
- Pogarsky, G., Roche, S. P., & Pickett, J. T. (2017). Heuristics and biases, rational choice, and sanction perceptions. *Criminology*, 55, 85–111.
- Ratner, K. G., Dotsch, R., Wigboldus, D. H. J., van Knippenberg, A., & Amodio, D. M. (2014). Visualizing minimal ingroup and outgroup faces: implications for impressions, attitudes, and behavior. *Journal of Personality and Social Psychology*, 106, 897–911.
- Reynald, D. M. (2009). Guardianship in action: developing a new tool for measurement. *Crime Prevention and Community Safety*, 11, 1–20.
- Reynald, D. M. (2010). Guardians on guardianship: factors affecting the willingness to monitor, the ability to detect potential offenders and the willingness to intervene. *Journal of Research in Crime and Delinquency*, (47), 358–390.

- Reynald, D. M. & Elffers, H. (2015). The routine activity of guardianship: comparing self-reports of guardianship intensity patterns with proxy measures. *Crime Prevention & Community Safety*, 17(4), 211–232.
- Reyns, B. W., Henson, B., & Fisher, B. (2011a). A situational crime prevention approach to cyberstalking victimization: preventive tactics for internet users and online place managers. *Crime Prevention and Community Safety*, 12, 99–118.
- Reyns, B. W., Henson, B., & Fisher, B. (2011b). Being pursued online: applying cyberlifestyle routine activities theory to cyberstalking victimization. *Criminal Justice and Behaviour*, 38, 1149–1169.
- Sampson, R. & Wooldredge, J. (1987). Linking the micro- and macro-level dimensions of lifestyle routine activity and opportunity models of predatory victimization. *Journal of Quantitative Criminology*, 3, 371–93.
- Simmons, A. D. & Bobo, L. D. (2015). When will nonprobability surveys mirror probability surveys? considering types of inference and weighting strategies as criteria for correspondence. *Sociological Methodology*, 45, 357–387.
- Simons, D. J. & Chabris, C. F. (2012). Common (mis)beliefs about memory: a replication and comparison of telephone and mechanical turk survey methods. *PLOS One*, 7(12), 1–5. doi:10.1371/journal.pone.0051876
- Sue, V. M. & Ritter, L. A. (2012). *Conducting online surveys*. Thousand Oaks, CA: Sage.
- Troll [Def. 6]. Retrieved September 30, 2016, from <http://www.collinsdictionary.com/dictionary/english/troll>
- Tsai, T. & Gill, J. (2013). Interactions in generalized linear models: theoretical issues and an application to personal vote-earning attributes. *Social Sciences*, 2, 91–113.
- U.S. Census Bureau Quick Facts. (2018). Retrieved from <https://www.census.gov/quickfacts/fact/table/US/PST045217>
- Vakhitova, Z. I. & Alston-Knox, C. L. (2018). Non-significant p-values? strategies to understand and better determine the importance of effects and interactions in logistic regression. *PLoS One*.
- Vakhitova, Z. I. & Reynald, D. M. (2014). Australian internet users and guardianship against cyber abuse: an empirical analysis. *International Journal of Cyber Criminology*, 8, 156–171.
- Vakhitova, Z. I., Reynald, D. M., & Townsley, M. K. (2016). Toward adapting routine activity and lifestyle exposure theories to account for cyber abuse victimization. *Journal of Contemporary Criminal Justice*, 32(2), 169–188.

- Vakhitova, Z. I., Webster, J. L., Alston-Knox, C. L., Reynald, D. M., & Townsley, M. K. (2018). The effect of offender-victim relationship and offender motivation on the utility of victims' online routine activities as risk factors: a mixed method analysis of cyber abuse crime events. *International Review of Victimology*, 24, 347–366.
- Vakhitova, Z. I., Alston-Knox, C. L., Reynald, D. M., & Townsley, M. K. (under review). Toward adapting lifestyle-routine activity theory to account for cyber abuse victimization: operationalization of main theoretical concepts.
- van Wilsem, J. (2013). Hacking and harassment—do they have something in common? comparing risk factors for online victimization. *Journal of Contemporary Criminal Justice*, 29, 437–453.
- Weinberg, J. D., Freese, J., & McElhatten, D. (2014). Comparing data characteristics and results of an online factorial survey between a population-based and a crowdsourcing-recruited sample. *Sociological Science*, 1, 292–310.
- Yar, M. (2005). The novelty of cybercrime. *European Journal of Criminology*, 2, 407–427.

Appendices

A Bayesian Profile Regression

In BPR, clusters of respondents with similar covariate profiles are formed through the application of a Dirichlet process prior and then associated with outcomes via a regression model (Molitor et al., 2010; Hastie et al., 2013; Mattei et al., 2016). Formally, in the case of categorical response data, we can specify the model as:

$$\text{logit}(p(Y_i = k \mid \theta_{Z_i}, \beta, W_i)) = \theta_{Z_i, k} + \beta_k W_i \quad \forall k = 1, 2, \dots, K-1$$

where K is the number of discrete levels in the response (in this analysis $K=4$), Z_i is the current profile allocation of individual i (estimated at each iteration), $\theta_{Z_i, k}$ are the profile (cluster) specific parameters for individual i and β_k are any overall fixed regression effects that may also be included in the model. In this analysis we do not have overall fixed effects for regression: instead, we use only cluster-specific parameters.

An important departure of the BPR approach from conventional regression methods is that the latter models the risk of individual participants, while the former infers the risk of groups of participants. The number of clusters is not fixed in advance; instead, it is explored throughout the algorithm. An estimation of the cluster-specific proportions for each category of cyber abuse victimization is given, and it is useful for understanding the main characteristics of each cluster. For example, one cluster may be characterized by a high probability of experiencing direct abuse and a much smaller probability of indirect abuse and an average probability of mixed abuse, while another cluster could be characterized by mixed abuse being the dominant method. To fit the BPR, we utilized R package PReMiuM version 3.1.4 (Liverani et al., 2015).

B Variable selection procedure

The following section describes the the procedure and the rationale behind the variable selection utilized in this study. Figures 4 and 5 show posterior inclusion probability distributions for *proximity to offenders* and *exposure to risk* variables. These figures show that, for example, participating in online gaming clearly contributes to the explanatory model with the median inclusion probability being greater than 90 per cent, however, posting comments on online newspapers—does not, with the

media inclusion probability being less than 10 per cent. Participating in online forums and posting about one's personal life online are not as clear cut in terms of contributing to the explanatory model, with the inclusion probabilities being almost uniformly distributed making them less informative in terms of the contribution to the explanatory model in this particular dataset. This does not mean we can discount the effect of these two variables completely, but in this dataset, we simply do not have enough information about the effect of these two variables to include them in the model.

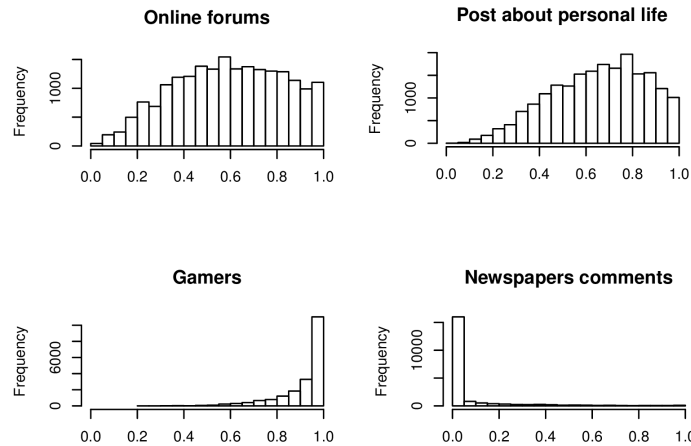


Figure 4: Posterior probability distributions of the importance of *proximity to offenders* variables based on 10,000 iterations of the Bayesian Profile Regression algorithm

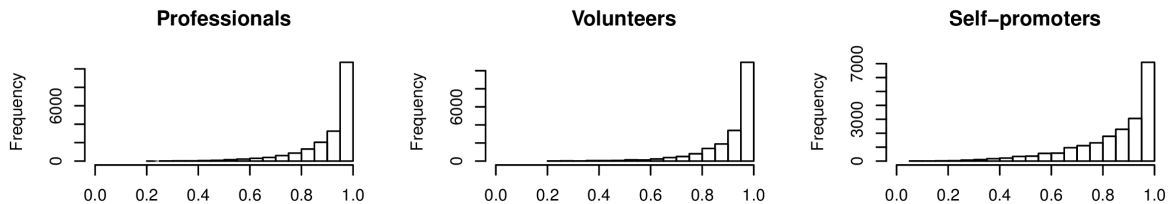


Figure 5: Posterior probability distributions of the importance of *exposure to risk* variables based on 10,000 iterations of the Bayesian Profile Regression algorithm

For example, to measure the effect of proximity to offenders, we have selected only online gaming, and left out using online forums, posting about one's personal life online and posting in the comments sections of online newspapers and social media (see Figure 4). In contrast, to measure exposure to risk, we have selected all three original variables: professional activities, volunteering, and self-promotion online (see Figure 5).

The variables we have excluded from the model were not necessarily unimportant, but they do not contribute as actively to the model as the selected variables. The selected variables (see Table 2)

were then used in modelling and further analyses using BPR.

ACCEPTED MANUSCRIPT

Notes

¹Cyber abuse is distinct from cyber bullying as the latter only involves victims under the age of 18.

²The survey was conducted in accordance with the ethical requirements of the Griffith University Human Research Ethics Committee (HREC) and complied with ethics guidelines set forth by the HREC recommendations. Ethics approval number: CCJ/07/14/HREC. Participants were informed that their data would be treated anonymously, no identifying information would be collected and they could withdraw from the survey at any time without providing a reason.

³Amazon's Mechanical Turk is an online contract labour portal <https://www.mturk.com/>

⁴Mechanical Turk is routinely used to recruit participants for research published in leading journals (Hitlin, 2016; Groenendyk, 2016; Pickett and Bushway, 2015; Pickett and Roche, 2017). Prior studies support the use of Mechanical Turk samples in academic research (Mullinix et al., 2015; Weinberg et al., 2014). For example, Mullinix et al. (2015) used Mechanical Turk and were able to replicate both the direction and the statistical significance of 29 (or 81%) of 36 treatment effects previously documented in probability samples of the American public. Pickett et al. (2018, p. 35) reviewed the use of Mechanical Turk in various types of social research and concluded that "across a variety of topics ... the use of an online convenience sample most often allows for accurate inferences about the direction and approximate magnitude of relationships between variables". For other reviews of the use of Mechanical Turk samples in different types of social research, see also Ansolabehere and Schaffner (2014), Brickman-Bhutta (2012), Dowling and Wichowsky (2014), Pasek (2016), Pogarsky et al. (2017), Ratner et al. (2014), Simons and Chabris (2012), and Simmons and Bobo (2015).

⁵Trolling is "post[ing] deliberately inflammatory articles on an internet discussion board" and being generally edgier than most (*Troll [Def. 6]*)

⁶As Table 3 suggests, the evidence supporting five clusters is the strongest, closely followed by the support for six clusters⁸. Support drops off considerably with 10 clusters having very weak support. Further investigation of the support for different numbers of clusters revealed that when six clusters are allocated, they are for the odd (extreme) values that do not fit the profile of any cluster particularly well.

Table 3: Support for different numbers of clusters

Number of clusters	5	6	7	8	9	10
Mean support	0.30	0.24	0.17	0.11	0.08	0.04

⁷Here, it is important to mention that the number of individuals who socialize with their ex-spouses in our sample is, not surprisingly, quite small ($n = 185$; 11.4%), so caution must be exercised when making any conclusions about this type of relationship.

Highlights:

- Lifestyle-routine activity theory appears useful for understanding different types of cyber abuse victimization
- Non-victims tend to be less involved in risky activities
- Proximity to offenders measured as online gaming is most consistently associated with cyber abuse
- Direct abuse is associated with less involvement in risky activities compared with indirect cyber abuse