*Article*

Crime & Delinquency
1–29

DOI: 10.1177/00111287241266589
journals.sagepub.com/home/cad


# A Latent Class Analysis of Online Victim-Offender Overlap among Chinese Youth: Examining Overlap Risks across Online Deviance Types

**Kai Lin[1], You Zhou[2], Boyang Xu[3], and Lennon Y. C. Chang[4]**

**Abstract**

This study aims to comprehensively test the applicability of lifestyle exposure theory (LET) against other criminogenic and victimogenic factors in predicting the differential risks of online offending-victimization overlap across multiple types of online deviance. Using self-reported survey data from 3,741 Chinese college students, the study performed Latent Class Analysis (LCA) and posterior multinomial logistic regression analysis. The LCA identified five latent classes of offending-victimization overlap, with only 6% of respondents reporting high overlap risk. Posterior multinomial logistic regression analysis showed that LET indicators and gender emerged as the most robust predictors of overlap risks compared to other theory-driven (e.g., control and routine activity theories) and sociodemographic

[1]University of Technology Sydney, Sydney, NSW, Australia
[2]Monash University, Melbourne, VIC, Australia
[3]China University of Political Science and Law, Beijing, China
[4]Deakin University, Melbourne, VIC, Australia

**Corresponding Author:**
You Zhou, School of Social Sciences, Faculty of Arts, Monash University, 21 Chancellors Walk, Clayton, Melbourne 3800, Australia.
Email: you.zhou@monash.edu

factors. The current study accentuates the importance of methodological diversity in examining victim-offender overlap.

**Keywords**
victim-offender overlap, online deviance, differential overlap risks, lifestyle theory, latent class analysis

## Introduction

The ubiquitous interactions between information and communication technologies (or ICT, which includes technologies such as the Internet, smartphones, social media, and artificial intelligence) and almost every level and aspect of our economic and social life have triggered the exponential growth of a wide variety of criminal activities in cyberspace, ranging from cyber fraud, phishing, hacking, identity theft, to online harassment/threat, blackmail, ransomware attack, etc. Indeed, online victimization has become one of the most common types of crime victimization in contemporary society. In the United States, for instance, the Internet Crime Complaint Center (IC3) received an average of over 552,000 reports of online victimization per year between 2016 and 2021; in 2021 alone, the financial losses reported by victims amounted to $6.9 billion (Internet Crime Complaint Center [IC3], 2022). Data from the NCVS Identity Theft Supplement report (Harrell, 2024) showed that in 2021, 12% of all Americans aged 16 or older were notified that an entity with their personal information experienced a data breach in the prior 12 months.

With the world's largest population of Internet users and the world's largest e-commerce market, China also battles the growing prevalence of online victimization in the country. In 2020, China recorded 927,000 cyber fraud cases alone, resulting in 35.37 billion Chinese yuan (roughly 5.44 billion US dollars) worth of financial losses (Wang, 2021).

In addition to cyber fraud and identity theft, cyber (sexual) harassment, cyberbullying, and online image-based abuse are also prevalent in both China and the US, especially among young people. For instance, a recent large-scale Chinese study estimated the prevalence rate of cyberbullying victimization among college students in China to be around 7.82% (Jin et al., 2023). In comparison, previous studies reported a prevalence ranging from 8.6% to 10% among college students in the US (Kraft & Wang, 2010; Schenk & Fremouw, 2012). A study of over 3,000 Internet users aged 15 and above in the US found that young people aged 15 to 29 were most likely to report online image-based abuse victimization, with 7% of Internet users under 30

experiencing this compared with 2% of adults aged 30 and older (Lenhart et al., 2016).

Since the early 2000s, criminologists have begun researching different domains of potential risk factors that predict the risk of online victimization. Other than demographic and socioeconomic characteristics (such as age, gender, and income), theoretical constructs such as routine online activity (e.g., Pratt et al., 2010; Reyns, 2015) and low self-control (e.g., Leukfeldt & Yar, 2016; Van Wilsem, 2013) have been given priority in empirical tests, and have been established in the current literature as prominent theoretical predictors of victimization risk for various kinds of online deviance. In recent years, however, mounting empirical evidence has begun to suggest that engagement in online deviance (such as cyberbullying, online sexual harassment, consuming online pornography, digital piracy, etc.) is a robust predictor of victimization (e.g., Choi et al., 2017; Holt & Bossler, 2008; Lin et al., 2023; Partin et al., 2022). Recent research has also consistently documented a substantial overlap between online offending and victimization in several populations (Burden, 2023; Kerstens & Jansen, 2016; Nodeland, 2020; Parti et al., 2022; Weulen Kranenbarg et al., 2019). These findings lend implicit support to lifestyle exposure theory (Hindelang et al., 1978), which argues that offending and victimization often overlap and that exposure to a deviant lifestyle (characterized by delinquent peer association, substance use, and other risky and illicit activities) elevates one's risk of victimization.

Nevertheless, there are several remaining gaps in this literature. First, extant research on online offending-victimization overlap has yet to assess the differential risks of overlap across heterogeneous types of online deviance. Second, existing research is yet to tease out nuanced elements of lifestyle exposure theory as applied to cyberspace and perform comprehensive tests of the theory against competing theoretical perspectives such as control and routine activity theories. Third, much of this research is also concentrated in the West, limiting the generalizability of their findings to the non-Western developing world, which is witnessing exponential growth in Internet use and cybercrime.

To model the tenets of lifestyle exposure theory and the characteristics of online offending and victimization accurately and comprehensively, the current study performs latent class analysis (LCA) and posterior regression analysis on survey data from over 3,700 youth in China. In particular, this study seeks to (a) identify latent classes of participating youth by their differential risks of offending-victimization overlap across online deviance types and (b) assess the applicability of lifestyle exposure theory in predicting the differential overlap risks in comparison with other criminogenic, victimogenic, and sociodemographic factors in the Chinese context.

## Co-occurring Offending and Victimization: Lifestyle Exposure Theory (LET)

As the leading theory of offending and victimization overlap, lifestyle exposure theory (LET) was first developed by Hindelang et al. (1978). The central tenet of LET is that an individual's expected social roles and position influence their lifestyles (characterized by the associated vocational and leisure activities), which, in turn, contribute to their risk of engaging in deviance *as well as* experiencing victimization. Among other propositions, this theory makes two distinct yet related empirical predictions: (a) offending often overlaps with victimization (offending-victimization overlap), and (b) a deviant lifestyle predicts an elevated risk of victimization (lifestyle-victimization link). Over the past few decades, LET has gained empirical support across many types of traditional crime (e.g., Cohen et al., 1981; Ferguson et al., 2023; Gottfredson& Grande-Bretagne, 1984; Nofziger, 2009; Sampson & Lauritsen, 1990).

In recent years, a growing number of empirical studies have tested these two empirical predictions of LET in the cyber context. Many studies examined offending-victimization overlap by dividing the research samples into a two-by-two victim-offender matrix: non-victim/offender, victim-only, offender-only, and victim-offenders. These studies typically asked the respondents about their offending and victimization experience with various online deviance, and a positive response to any type of offending or victimization would qualify the respondent as a victim or offender. For example, Kerstens and Jansen (2016) drew on self-reported survey data from 6,299 Dutch youth. They found that the online victim-offender overlap was substantial across different types of financial cybercrime. The victim-offender subgroup was significantly associated with low self-control, retaliation, and online disinhibition. Weulen Kranenbarg et al. (2019) examined a Dutch sample of high-risk adult suspects of cybercrime and traditional crime and found 9.59% victim-offender overlap for cybercrime and 13.73% for traditional crime. They further suggested that correlates like low self-control and routine activities partly explained victim-offender overlap in cybercrime. A more recent study (Nodeland, 2020) analyzed a sample of university students in the southern US and found that low self-control and online delinquent peer association predicted a higher risk of victimization-offending overlap. Similarly, a national study of US adult Internet users by Burden (2023) found that 16.6% of the research participants identified as victim-offenders of cybercrime and that compared to those who did not report either offending or victimization, victim-offenders were more likely to be male, younger, and exhibited low self-control.

Other studies have analyzed the correlation between online offending and victimization and tested the lifestyle-victimization link. For instance, Holt and Bossler (2008) found that engaging in computer-based deviance (e.g., digital piracy, online pornography, and hacking) significantly increased the risk of experiencing online victimization. Choi et al.' (2017) study of US college students found that respondents who engaged in risky online leisure activities were more likely to experience interpersonal violence in cyberspace. More recently, Partin et al. (2022) found that engagement in 14 risky online behaviors (e.g., sending personal information to unknown people online) significantly predicted 15 forms of online victimization, such as hacking, phishing email, cyberbullying, online harassment, online scam, and online stalking among US college students. Lin et al. (2023) recent study of Chinese university students also identified a similar link between online deviance and cyber fraud victimization.

## Criminogenic Factors of Online Offending: Delinquent Peers, Self-Control, and Social Bonds

While LET provides an appropriate theoretical framework for explaining online offending-victimization overlap, other criminological theories have been applied to understanding the etiology of standalone online offending. For instance, social learning theory and its predecessor, differential association theory (Akers & Jennings, 2019; Sutherland, 1947), have been widely adopted by empirical studies of online deviance. Both theories postulate that individuals acquire deviance through associating with delinquent peers. Studies in cyberspace have found that delinquent peers play a critical role in encouraging an individual's online deviance involvement, including digital piracy, hacking, cyberbullying, online harassment, and online pornography (e.g., Gunter, 2008; Higgins & Makin, 2004; Holt et al., 2012; Li et al., 2016; Zhou et al., 2024). Studies have also found that offline delinquent peers had a greater influence than virtual peers in predicting online deviance perpetration (Dearden & Parti, 2021; McCuddy, 2021; Weulen Kranenbarg et al., 2019). A more recent study by Zhou et al. (2024) found traditional social learning (learning from offline delinquencies) can exert equivalent effect on cyber deviance compared to online social learning (learning from online delinquencies), indicating the offending versatility potential of delinquent peer association.

Low self-control is another robust correlate of online deviance. Self-control theory posits that individuals' criminal activities result from their inability to delay instant gratifications and resist illegitimate and illegal means of gratifications (Gottfredson & Hirschi, 1990). The theorists portrayed individuals

with lower levels of self-control as "impulsive, insensitive, physical, risk-seeking, short-sighted, and non-verbal" (Gottfredson & Hirschi, 1990). Previous research has widely established low self-control as a crucial predictor of traditional delinquent and criminal activities (e.g., Burt, 2020; Pratt & Cullen, 2000), and the cybercrime literature also provides strong evidence for the significant relationship between self-control and a wide range of online deviant behaviors (e.g., Choi et al., 2017; Holt et al., 2012; Li et al., 2016). Studies have also demonstrated the cross-population robustness of self-control in explaining online deviance. For example, Choi and Lee (2017) drew on a sample of 715 Korean middle school students and found that low self-control was a significant factor associated with online sexual harassment. B. Xu et al. (2021) found that low self-control significantly predicted Chinese juveniles' online delinquency even after controlling for the mediation effect of delinquent peers.

Unlike differential association and self-control theories, social bonds theory has received less attention among cybercrime scholars. Social bonds theory, also known as social control theory, argues that individuals' bonds with conventional social institutions (e.g., parents, partners, friends, schools, communities, religions, etc.) can reduce their odds of committing crimes (Hirschi, 1969). Antecedent studies have demonstrated the applicability of social bonds theory in explaining a variety of traditional delinquency and crime (e.g., Sampson & Laub, 1990; Stack et al., 2004). Nevertheless, only a handful of empirical studies have fully operationalized social bonds and explored their relationships with online offending. One of these studies (Stack et al., 2004) analyzed self-reported survey data from 531 US Internet users and found that religious and marital bonds were significant deterrents to consuming online pornography. More recently, Back et al. (2018) examined survey data of 18,985 students from eight countries and suggested that parental supervision and school attachment were significantly and negatively associated with juvenile hacking. However, the significant relationships varied across the countries in the study, justifying further cross-population comparison.

## Victimogenic Factors of Online Victimization: Routine Activities, Self-Control, and Sociodemographic Characteristics

Similarly, extant literature has identified several domains of risk factors across multiple types of cyber victimization, including online routine activities, low self-control, and demographic and socioeconomic factors. Studies

have indicated the theoretical potential of routine activity theory in examining online victimization. Routine activity theory suggests that crime occurs when suitable targets, motivated offenders, and the absence of capable guardians converge spatially and temporally (Cohen & Felson, 1979). Although the theory originally posited the victimogenic etiology in terrestrial contexts, multiple empirical studies have documented the applicability of routine online activity in understanding online victimization risk. Pratt et al. (2010) study examined attempted cyber fraud using a representative sample from a state-wide survey in the US. They found that indicators of routine online activity fully mediated the effect of sociodemographic characteristics on the likelihood of being targeted for fraud online. A more recent study (Mesch et al., 2018) from the US also found that the risk of being targeted with a fraudulent offer is associated with low self-control and online routine activities. Leukfeldt and Yar's (2016) study of a large Dutch sample revealed that some elements of routine online activity theory were more applicable than others. Visibility plays a role in online victimization, while accessibility and having personally capable guardianship showed inconsistent effects. Furthermore, value and having technically capable guardianship showed almost no effects on online victimization. Reyns' (2015) study of the general Canadian population found that particular online behaviors, including booking/making reservations, social networking, and having one's information posted online, were consistently and positively related to being targeted for all three types of online victimization. Lin et al. (2023) study of Chinese university students found that routine online activities only predicted a higher risk of experiencing attempted but not completed online fraud victimization.

Many studies of online victimization have also identified a clear link between the psychological trait of low self-control and high victimization risk (Bossler & Holt, 2010; Lin et al., 2023; Mesch et al., 2018; Partin et al., 2022; Reyns et al., 2019; Van Wilsem, 2013). For instance, Reyns et al. (2019) studied a sample of US college students. They discovered that low self-control was significantly predictive of online victimization in situations where victimization depended heavily on individual decisions. Similarly, Lin et al. (2023) found that low self-control only predicted higher odds of completed, but not attempted, online fraud victimization. Furthermore, several studies have also identified a mediating effect of online activities on the relationship between low self-control and elevated online victimization risks. For example, using a representative sample of the Dutch population, Van Wilsem (2013) revealed that active online shoppers, those who participated in online forums, and those with low self-control ran substantially higher victimization risks. Furthermore, routine online activities partially mediated the connection between self-control and victimization.

Demographic and socioeconomic characteristics have also been identified as significant correlates of online victimization. Among the demographic factors, age is associated with online victimization, although the findings are not consistent across samples from different countries. In North America, multiple studies have documented a positive effect of age on the victimization risk of cybercrime (Mesch & Dodel, 2018; Partin et al., 2022; Pratt et al., 2010; Reyns, 2015). In China and Europe, however, studies have demonstrated a negative effect of age on online victimization risk (Leukfeldt & Yar, 2016; Lin et al., 2023; Van Wilsem, 2011, 2013). Indeed, official statistics from the US identify older adults as a vulnerable group for online victimization (Internet Crime Complaint Center [IC3], 2022), whereas regulatory bodies in China and Europe have pointed to the younger generation as the more at-risk group (China Academy of Information and Communications Technology [CAICT], 2020; European Commission, Directorate-General for Migration and Home Affairs, 2020). This may be attributed to the different targeting strategies by offenders in these regions. Moreover, gender is also an important demographic factor affecting online victimization risk. In all the studies mentioned above, men and boys seem to be at higher risk of online victimization than women and girls (Leukfeldt & Yar, 2016; Lin et al., 2023; Mesch & Dodel, 2018; Partin et al., 2022; Pratt et al., 2010; Reyns, 2015; Van Wilsem, 2011, 2013).

Apart from demographic characteristics, socioeconomic characteristics such as income and education have also been examined as predictors of online victimization odds, and the literature shows mixed findings, often depending on the specific crime type. For instance, using data from Canada's General Social Survey, Reyns (2015) examined three types of online victimization (phishing, hacking, and malware infection victimization). They found that income positively predicted phishing and malware victimization but negatively predicted hacking victimization. Pratt et al. (2010) US study did not find a significant effect of income or education on the odds of cyber fraud targeting after controlling for routine online activities. Leukfeldt and Yar's (2016) Dutch study found that education slightly increases, while personal income slightly decreases the odds of malware victimization; education was also found to reduce the odds of consumer fraud slightly. Another Dutch study utilized a nationally representative sample and found a positive effect of age on cyber fraud victimization (Van Wilsem, 2013) but a null effect of education on digital threat victimization (Van Wilsem, 2011).

## Online Offending and Victimization in China

As discussed previously, online offending and victimization are prevalent in China, and they reflect the economic and social realities of contemporary

Chinese society. For instance, in contrast to cyber fraud victims in the United States, most of whom were adults 40 and older (Internet Crime Complaint Center [IC3], 2022), victims of cyber fraud in China were primarily from the younger population, with 63.7% of those recently defrauded born after 1990 (China Academy of Information and Communications Technology (CAICT), 2020). The preponderance of youthful victims in cybercrime victimization in China may reflect the rapidly shifting landscape of routine activities, principally driven by young Internet users. A recently published report shows that in 2021, retail e-commerce sales constituted 52.1% of total retail sales in China, up from only 34% in 2019, and is projected to reach 58.1% in 2024 (Cramer-Flood, 2021). The fast adaptability of young Chinese consumers regarding online behaviors is also illustrated by their willingness to try out new modalities of online shopping. Customers of retail e-commerce featuring live streaming (on platforms such as *Douyin*, the Chinese version of TikTok) represented 38.8% of all digital buyers in 2021, up from only 19% in 2019 (Cramer-Flood, 2021). Over 40% of those who shopped by watching live-streamed advertisements were young people born after 1990 (Zhuang, 2020). As "natives" of cyberspace, the younger population in China is especially exposed to this increasingly complex cyber environment conducive to both online offending and victimization (Y. Xu, 2022).

Over the past few years, there has been a growing body of literature on cybercrime in China, and much of this research is focused on offending. For instance, a recent study by Zhou et al. (2024) suggested traditional social learning can exert similar effects on cyber deviance compared to online social learning among Chinese youth. Chen (2021) analyzed 20 fraudulent conversations intercepted by law enforcement and found repeated patterns of conversation skills used by the fraudsters to trigger the victims' psychological panic. Y. Xu and Xu (2021) examined 18 court adjudications in Zhejiang Province and found that cross-border telecom and cyber fraud is not simply a low-risk-high-return endeavor; the risks and potential return vary noticeably across different groups of offenders. Lee's (2021) study of Baidu Tieba, a Chinese version of Craigslist, revealed that the methods and virtual platforms for perpetrating cyber fraud in China had evolved over the years, reflecting the rapid technological transformation of Chinese society in the past decade. Research on online victimization is relatively sparse and typically only focused on cyber fraud. For instance, a recent empirical study of cyber fraud victimization was conducted by Y. Xu (2022), who interviewed 30 cyber fraud offenders and 23 fraud victims. He found that most victims' personal information has been stolen and used to construct a tailored "con-script" against them. Lin et al. (2023) recent study on online victimization was also limited to cyber fraud alone.

## Current Study

As discussed in the literature review, despite a robust and growing body of criminological literature on online offending and victimization, there are several theoretical and empirical gaps. First of all, studies that explicitly examined victim-offender overlap (Burden, 2023; Kerstens & Jansen, 2016; Nodeland, 2020; Parti et al., 2022; Weulen Kranenbarg et al., 2019) typically classified an individual as a victim or offender if they had reported offending or victimization of *any* type of online deviance. Extant research has yet to identify the potential clustering of offenders, victims, and offender-victims across online deviance types (e.g., "generalist" vs. "specialist" offenders, victims, and offender-victims) and explore their associated characteristics. Similarly, current research on the lifestyle-victimization link (Choi et al., 2017; Holt & Bossler, 2008; Lin et al., 2023; Nodeland, 2020; Partin et al., 2022) has yet to assess whether the link would hold across different groups of individuals exhibiting disparate levels of offending, victimization, and overlap risk by online deviance type. In addition, few studies have systematically operationalized deviant lifestyle exposure in consideration of these nuances and investigated its effect against a wide range of other well-established criminogenic and victimogenic factors. Finally, no study has examined online offending-victimization overlap in China, a country with the world's largest population of Internet users and the world's largest e-commerce market, and a growing incidence of online offending and victimization.

Adopting Latent Class Analysis (LCA), the current study is intended to model and test LET as extended to cyberspace with a sample of over 3,700 Chinese youth. The first objective of this study is to identify latent classes of participating youth by their risk of offending-victimization overlap across online deviance types. Furthermore, the current study sets out to assess the efficacy of deviant lifestyle exposure in predicting online offending-victimization risks and patterns as compared to other well-established criminogenic and victimogenic factors (i.e., online routine activities, self-control, social bonds), controlling for relevant sociodemographic characteristics (age, gender, family economic status, etc.). The following hypotheses were thus formulated and tested in this study:

$H_1$: Online offending-victimization overlap is prevalent among those reporting offending or victimization.

$H_2$: Online offending-victimization overlap across multiple types of online deviance (i.e., multimodal overlap) is prevalent among those reporting offending or victimization.

$H_3$: Deviant lifestyle exposure strongly predicts online victimization (including offending-victimization overlap) above and beyond other criminogenic, victimogenic, and sociodemographic factors.

## Data Collection and Procedure

Self-reported survey data was collected in October 2020 at a college (equivalent to a junior college in the US) in a mid-sized Chinese city. After the survey questionnaire was developed, it was first translated from English to Chinese and back-translated to English by two certified translators, ensuring the meaning of the survey items was not biased by language and culture (Brislin, 1970). The Ethics Committee of a co-author's affiliated university thoroughly reviewed and approved the research proposal before initiating data collection. All students enrolled in the college were invited to participate in the study. The research team came to the classes and solicited student participation. The researchers explained to the students the purpose of the study and how to participate in the study. They also clarified the voluntary and anonymous nature of the student's participation and ensured that data would only be analyzed and reported in an aggregate manner. All voluntary participants were notified to bring at least one digital device with a stable Internet connection on the data collection date. Each class was slotted 45 min to complete the questionnaires in a separate classroom on the data collection date. Informed consent was obtained before participating in the research, with parental approval for participants under 18.

The survey questionnaires were administered via Sojump (问卷星), an online survey software that can be embedded in Chinese mainstream social media platforms. In Sojump, participants can be automatically notified about missing responses, minimizing the probability of missing values in the dataset. By clicking the online questionnaire link, students could complete the online questionnaires on their digital devices (e.g., mobile phones, tablets, and laptops). A trial study was conducted to ensure the students fully understood the meaning of the questionnaires. In total, 4,209 online surveys were distributed to the students, and 3,825 surveys were returned, resulting in a response rate of 90.9%. The response rate is relatively high for two reasons. First, the survey was easily accessible from any electronic device, encouraging participation. Second, the school administrative board arranged a specific time slot for the research team to collect data. This means the students were provided adequate time and space to complete the online questionnaire, boosting the response rate. After listwise deleting the cases with missing values in the dependent variables, the final sample size registered at 3,741.

## Measures

### Online Offending

Six types of online offending were measured in the study. Respondents were asked how often they had done the following: "harassing others online," "sexually harassing others online," "threatening or abusing others with violence online," "hacking into others' private accounts," "downloading illegal or pirated software," and "sending sexually explicit images to others without approval" (0 = never to 3 = often). These items were dichotomized into a series of dummy variables, with 0 denoting "never" and 1 representing having perpetrated online deviance.

### Online Victimization

Six common types of online victimization were measured in the survey instrument. Respondents were asked how often they had experienced the following: "having their private information exposed," "having their identity hacked," "having been bullied verbally online," "having been sexually harassed online," and "having experienced cyber fraud," and "having their online accounts stolen" (0 = never to 3 = often). These items were dichotomized into a series of dummy variables, with 0 denoting "never" and 1 denoting having experienced online victimization.

### Deviant Lifestyle Exposure

Lifestyle was operationalized by four demographic factors (age, race, income, and marital status) in Hindelang et al.'s (1978) original study, which was subsequently criticized (Engström, 2021; Gottfredson, 1981; Pratt & Turanovic, 2016). Recent studies departed from the original approach by implementing various operations in measuring deviant lifestyles, including illegal activities, victimization, delinquent peer associations, substance abuse, and other risky (but not illegal) events (see Engström, 2021). In this study, involvement in a deviant lifestyle was measured by delinquent peer association (offline and online), offline delinquency, and disclosure of personal information online. Delinquent peer association (offline deviance) was measured by how many of the respondent's friends had engaged in any of the following offline delinquency in the past 12 months: (a) skipping classes, (b) physical fights, (c) excessive drinking, and (d) committing a crime (0 = none of my friends to 4 = all of my friends). Delinquent peer association (online deviance) was measured by how many of the respondent's friends had

engaged in the following online delinquency in the past 12 months: (a) illegally downloading music and software, (b) attempting to guess or crack other people's social media accounts, (c) taking revenge on others using social media, and (d) checking or using other people's electronic devices without their permission (0 = none of my friends to 4 = all of my friends). With a respective Cronbach alpha coefficient of .89, indicating excellent interitem reliability, the items were summed into two additive indices. Offline delinquency was measured by the respondent's weekly frequency of: (a) excessive drinking (1 = no drinking to 8 = seven times or more), (b) smoking (1 = no smoking to 4 = five or more days a week), (c) going to social gatherings (1 = no time to 8 = seven times or more), (d) night clubs or bars (1 = no time to 8 = seven times or more). Online self-information disclosure was measured by whether the respondent had disclosed their real names, real information about their family or friends, information about their dating or friending preferences, mobile number, email address, and other social media handles (0 = never to 3 = often). With a Cronbach alpha coefficient of .92, indicating excellent interitem reliability, the items were summed into an additive index.

### *Self-control (impulsivity) and Social Bonds*

Impulsivity and social bonds were also measured. Impulsivity was measured by four items. Respondents were asked the extent to which they agree (1 = completely disagree to 4 = completely agree) with the following statements: "I usually do things without thinking about it," "I seldom think about my future," and "I often do things that bring me instant gratification even if they may be harmful in the long term" "I focus more on things that are about to happen rather than things that will happen to me in the distant future." With a Cronbach alpha coefficient of .79, indicating good interitem reliability, the items were summed into an additive index. Parental bond was measured by the respondent's degree of agreement (1 = completely disagree to 4 = completely agree) with the following statements: "My parents will help me when I am in trouble," "I can talk about my future goals and plans with my parents," "I can share my thoughts and feelings with my parents," "I respect my parents a lot," and "I enjoy spending time with my parents." With a Cronbach alpha coefficient of .89, indicating excellent interitem reliability, the items were summed into an additive index. School bond was measured by the respondent's degree of agreement with the following statements: "I love going to school," "Getting good grades is important," and "I put much effort into studying." With a Cronbach alpha coefficient of .87, indicating excellent interitem reliability, the items were summed into an additive index.

### *Online Routine Activities and Low Social Media Guardianship*

Online routine activities were measured by five items: time spent on the Internet every day (1 = less than 1 hr to 9 = more than 8 hr), number of social media accounts (1 = no account to 9 = eight accounts), number of social media posts every week (1 = no time to 8 = seven times and more), number of photos uploaded to social media (1 = zero to 10 = 41 and more photos), and number of followers on social media (1 = fewer than 50 people to 11 = 501 people and more). Low social media guardianship was operationalized as an index of four survey items: to what extent you will agree to: (a) strangers visiting your social media, (b) adding new friends via algorithm recommendation, (c) making your social media visible only with your permission, and (d) displaying information on who had visited your social media (1 = definitely won't to 4 = definitely will). With a Cronbach alpha coefficient of .71, indicating good interitem reliability, the items were summed into an additive index.

### *Sociodemographic Characteristics*

Gender was measured by a binary variable with 0 denoting "male" and 1 denoting "female." Household registration (i.e., *hukou*) status was measured by a dummy variable (0 = rural household and 1 = urban household. Academic rank was measured by a five-point scale, with 5 being "top tier of class" and 1 being "bottom tier of class." Income was measured by the survey item "How much is your family's monthly income?" The response categories ranged from 1 = "1,000 yuan and less" to 6 = "5,001 yuan and more." Table 1 summarizes the descriptive statistics of all variables.

## Analytic Strategy

The data of the current study was analyzed in two steps. First, Latent Class Analysis (LCA) was performed on the six dummy variables of online offending and victimization to derive the best-fitted number of latent classes. Next, based on the results of the LCA, a multinomial logistic regression model was estimated to compare the criminogenic, victimogenic, and other relevant sociodemographic characteristics across latent classes.

LCA is a statistical technique used for qualitatively identifying different subgroups within populations that often share certain outward characteristics (Hagenaars & McCutcheon, 2002). The assumption underlying LCA is that membership in unobserved groups (or latent classes, as they are referred to in LCA) can be explained by patterns of scores across survey questions, assessment indicators, or scales (Weller et al., 2020). Compared to the commonly adopted gross dichotomization approach, LCA has the advantage of

**Table 1.** Descriptive Statistics ($N = 3,741$).

| Variables | Mean | Std | Min | Max |
|---|---|---|---|---|
| Age | 19.28 | 1.22 | 16 | 24 |
| Female | .28 | .45 | 0 | 1 |
| Parental income | 2.99 | 1.64 | 1 | 6 |
| Class rank | 3.42 | .99 | 1 | 5 |
| Urban household | .18 | .38 | 0 | 1 |
| Harassing others online | .24 | .43 | 0 | 1 |
| Sexually harassing others online | .18 | .38 | 0 | 1 |
| Threatening or abusing others online | .17 | .38 | 0 | 1 |
| Hacking into others private accounts | .14 | .35 | 0 | 1 |
| Illegally downloading pirated software | .17 | 37 | 0 | 1 |
| Sending sexually explicit images to others | .15 | .35 | 0 | 1 |
| Private information exposed | .08 | .28 | 0 | 1 |
| Identity hacked | .07 | .26 | 0 | 1 |
| Bullied online | .14 | .34 | 0 | 1 |
| Sexually harassed online | .11 | .31 | 0 | 1 |
| Defrauded online | .14 | .35 | 0 | 1 |
| Online accounts stolen | .22 | .41 | 0 | 1 |
| Offline delinquent peer associations | 1.32 | 2.67 | 0 | 16 |
| Online delinquent peer associations | 1.53 | 2.92 | 0 | 16 |
| Offline delinquency | 6.26 | 3.45 | 4 | 28 |
| Disclosure of personal information | 3.98 | 4.60 | 0 | 27 |
| Impulsivity | 7.02 | 2.55 | 4 | 16 |
| Parental bond | 15.40 | 3.94 | 5 | 20 |
| School bond | 8.99 | 2.49 | 3 | 12 |
| Time spent online | 3.91 | 2.29 | 1 | 9 |
| Number of social media accounts | 4.56 | 1.78 | 1 | 9 |
| Number of social media posts every week | 2.27 | 1.61 | 1 | 8 |
| Number of photos uploaded to social media | 2.96 | 2.62 | 1 | 10 |
| Number of social media followers | 3.52 | 3.14 | 1 | 11 |
| Low social media guardianship | 9.04 | 2.90 | 4 | 16 |

transcending *a priori* categories of the victim-offender matrix and inductively identifying latent classes emerging from the data.

## Results

The results show that 2, 3, 4, 5, 6, and 7-class LCA models were fitted, as well as Goodness of Fit Indices, including Kaike's Information Criterion (AIC), Schwarz's Bayesian Information Criterion (BIC), Likelihood Ratio

Chi-Squares, and entropy were calculated. Table 2 summarizes the Goodness of Fit Indices across the LCA models. As is demonstrated in Table 2, the 4-class and 5-class models exhibited the best model fit and were therefore adopted for further analysis. The two models were not substantially different—three latent classes were almost identical. Results from the 5-class model are presented as they yield the most profound empirical and theoretical insights.

Figure 1 summarizes the number of cases in each of the five latent classes and the proportion of different types of online offending and victimization in each latent class. Latent Class 1 (LC 1) comprises 71.0% of the entire sample, and the respondents in LC1 reported minimal risks of online offending or victimization. Latent Class 2 (LC 2), comprising 6.7% of the entire sample, consists of respondents who had reported a medium risk of multimodal online offending and a relatively low risk of online victimization. Latent Class 3 (LC 3), comprising 6.4% of the total sample, is composed of respondents with high risks of multimodal online offending and minimal risks of online victimization. Latent Class 4 (LC 4), which makes up 9.9% of the total sample, is made up of respondents with low risks of online offending and medium risks of multimodal online victimization. Latent Class 5 (LC 5) occupies 6% of the sample, comprising respondents with high risks of multimodal offending-victimization overlap.

Next, a multinomial regression model was estimated to compare the effects of the research variables on the odds of being in LC 2 to LC 5 versus LC 1 (baseline group), as is shown in Table 3. The likelihood ratio chi-square [$\chi^2$ (72)=2211.86; Prob$>\chi^2$=0.0000] suggests that the model as a whole fits significantly better than an empty model (i.e., a model with no predictors). The McFadden Pseudo $R^2$=.31 indicates good explanatory power of the model. Relative risk ratios (i.e., odds ratios) were reported for each independent variable in the models. Maximum and mean Variance Inflation Factors (VIFs) were calculated and reported. Both were well below the established threshold of 5 or 10 (James et al., 2013), suggesting multicollinearity is not a concern in the model.

Results in Comparison 1 (LC 2 vs. LC 1) reveal that, as compared to male students, female students exhibit 70% lower log odds of being in LC 2. With each additional unit increase in delinquent peer associations (online deviance), offline deviance, personal information disclosure, and impulsivity, the students demonstrate 17%, 9%, 40%, and 14% higher log odds of being in LC 2. With each unit increase in school bond, the students show 9% lower log odds of being in LC 2.

In Comparison 2 (LC 3 vs. LC 1), female students have 45% lower log odds of being in LC 3. An increase of every unit in delinquent peer associations (online deviance), offline deviance, personal information disclosure, and impulsivity predicts 25%, 13%, 60%, and 13% higher log odds of being in LC 3. However, with each unit increase in the number of photos uploaded to social media and low social media guardianship, the students indicate 14% and 10% lower log odds of being in LC 3.

**Table 2.** Goodness of Fit Indices for LCA ($N = 3{,}741$).

| Indices | 2 class | 3 class | 4 class | 5 class | 6 & 7 class |
|---|---|---|---|---|---|
| Likelihood ratio chi-square[†] | $\chi^2$ (4,070) = 5812.595** | $\chi^2$ (4,057) = 4243.164* | $\chi^2$ (4,044) = 2022.968 | $\chi^2$ (4,031) = 1685.204 | Could not converge |
| AIC | 26044.873 | 24501.443 | 22307.246 | 21995.483 | |
| BIC | 26200.551 | 24738.073 | 22624.829 | 22394.018 | |
| Entropy | .96 | .92 | .94 | .92 | |

[†]The null hypothesis states that the model fits as well as the saturated model.
*$p < .05$. **$p < .01$

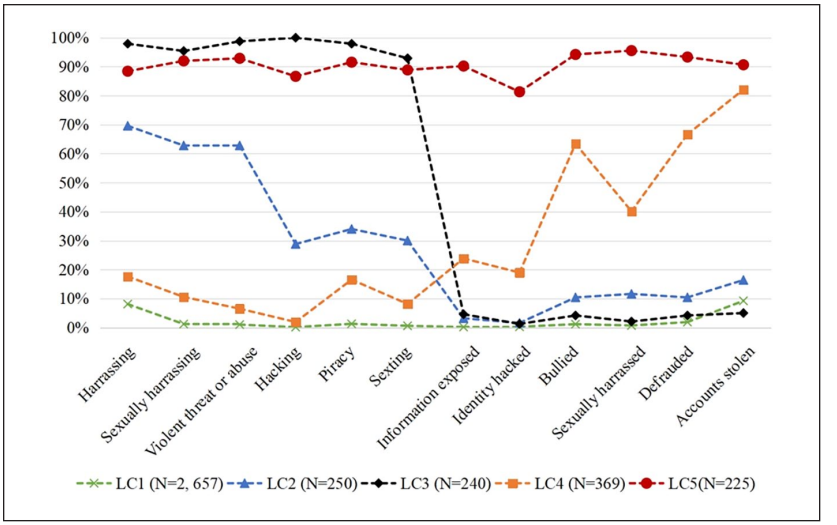


**Figure 1.** The prevalence of online offending & victimization by latent classes ($N = 3{,}741$).

*Notes.* The proportion indicates to what extent the individuals in each latent class had experienced each online offending and victimization.

LC1: Minimal offending and victimization

LC2: Medium multimodal offending and low victimization

LC3: High multimodal offending and minimal victimization

LC4: Low offending and medium multimodal victimization

LC5: High multimodal offending and high multimodal victimization.

In Comparison 3 (LC 4 vs. LC 1), female students have 50% lower log odds of being in LC 4. With each additional unit increase in delinquent peer associations (offline deviance), delinquent peer associations (online deviance), offline deviance, personal information disclosure, impulsivity, and time spent online, the students show 20%, 8%, 8%, 12%, 10%, and 14% higher log odds of being in LC 4. Nevertheless, with each unit increase in school bond and the number of social media posts every week, the students exhibit 9% and 7% lower log odds of being in LC 4.

The results in Comparison 4 (LC 5 vs. LC 1) suggest that female students have 78% lower log odds of being in LC 5. With each additional unit increase in delinquent peer associations (offline deviance), delinquent peer associations (online deviance), offline deviance, personal information disclosure, and impulsivity, the students show 26%, 21%, 21%, 56%, and 18% higher log odds of being in LC 5. In contrast, with each unit increases in parental bond, school bond, and low social media guardianship, the students exhibit 10%, 10%, and 9% lower log odds of being in LC 5.

**Table 3.** Multinominal Logistic Regressions on the Latent Classes ($N = 3{,}741$).

| Variables | Comparison 1 | | Comparison 2 | | Comparison 3 | | Comparison 4 | |
|---|---|---|---|---|---|---|---|---|
| | LC2 vs. LC1 | | LC3 vs. LC1 | | LC4 vs. LC1 | | LC5 vs. LC1 | |
| Independent variables | *OR* | *SE* | *OR* | *SE* | *OR* | *SE* | *OR* | *SE* |
| Lifestyle-exposure factors | | | | | | | | |
| Delinquent peer associations (offline deviance) | 1.06 | .05 | 1.02 | .04 | 1.20** | .04 | 1.26** | .06 |
| Delinquent peer associations (online deviance) | 1.17** | .04 | 1.25** | .05 | 1.08* | .04 | 1.21** | .05 |
| Offline deviance | 1.09** | .03 | 1.13** | .03 | 1.08** | .02 | 1.21** | .03 |
| Disclosure of personal information | 1.40** | .03 | 1.60** | .04 | 1.12** | .02 | 1.56** | .04 |
| Criminogenic and victimogenic factors | | | | | | | | |
| Impulsivity | 1.14** | .04 | 1.13** | .04 | 1.10** | .03 | 1.18** | .05 |
| Parental bond | .99 | .03 | .96 | .03 | 1.02 | .02 | .90** | .03 |
| School bond | .91* | .04 | .95 | .04 | .91** | .03 | .90* | .05 |
| Time spent online | 1.06 | .04 | .96 | .04 | 1.14** | .03 | .99 | .05 |
| Number of social media accounts | .96 | .05 | .95 | .05 | .93* | .04 | .91 | .05 |
| Number of social media posts every week | .90 | .05 | 1.11 | .06 | .95 | .04 | .95 | .06 |
| Number of photos uploaded to social media | .97 | .03 | .86** | .04 | .99 | .03 | .94 | .04 |
| Number of social media followers | .96 | .03 | .98 | .03 | .99 | .02 | .97 | .03 |
| Low social media guardianship | .95 | .03 | .90** | .03 | 1.02 | .02 | .91* | .04 |
| Demographic and socioeconomic factors | | | | | | | | |
| Age | .93 | .06 | 1.14 | .08 | .98 | .05 | 1.06 | .09 |
| Female | .30** | .07 | .55** | .13 | .50** | .08 | .22** | .07 |
| Parental income | .96 | .04 | 1.02 | .05 | .99 | .04 | 1.01 | .06 |
| Class rank | 1.05 | .08 | .99 | .09 | .98 | .06 | .93 | .09 |
| Urban household | 1.02 | .19 | .66 | .16 | .94 | .15 | .59 | .16 |
| Likelihood ratio chi-square | $\chi^2$ (72) = 2311.86** Pseudo $R^2$ = .31 | | | | | | | |
| Maximum/mean VIF | 3/1.53 | | | | | | | |

*Note.* *OR* = Odds Ratio; *SE* = Standard Error.
*$p < .05$. **$p < .01$.

## Discussion and Conclusion

Implementing LCA, the current research divided 3,741 participating youth in China into five latent classes, each exhibiting a different risk of offending and victimization across various types of online deviance. The results showed that excluding those reporting minimal offending and victimization, 20.7% of the remaining participants (6.0% of the total sample) reported a high risk of offending-victimization overlap across a wide range of online deviance. An additional 50.1% of the remaining participants reported some offending-victimization overlap, although the risk level was lower, and the overlap was concentrated in several types of online deviance. Thus, Hypothesis 1 is accepted, but Hypothesis 2 cannot be accepted. Posterior multinomial logistic regression analysis showed that other than gender, deviant lifestyle exposure (characterized by delinquent peer associations, risky online behaviors, and offline delinquency) was consistently *the strongest* predictor of latent class membership, supporting Hypothesis 3. Considering other established criminogenic and victimogenic factors, impulsivity consistently predicted latent class membership across all comparisons, while social bonds and routine online activities demonstrated *domain specificity*—each factor is associated with one or two latent classes of offenders and/or victims.

These findings necessitate further unpacking. Theoretically, findings from the present study lend support to both empirical predictions of LET (i.e., offending-victimization overlap and the lifestyle-victimization link) and add nuances to these predictions in the online context. In the current sample of Chinese youth, online offending-victimization overlap, if defined broadly, is common. In fact, the LCA did not yield strictly "offender-only" and "victim-only" latent classes. However, high-risk multimodal (i.e., "generalist") overlap only made up a fraction (6%) of the total sample. This finding slightly contrasts those from previous research identifying overlap with the victim-offender matrix (e.g., Burden, 2023; Kerstens & Jansen, 2016; Nodeland, 2020; Parti et al., 2022; Weulen Kranenbarg et al., 2019), which reported between 9.59% and 51.2% of victim-offender overlap. This is because the qualifying threshold for "victim-offender" is low under the dichotomous categorization paradigm, as it only requires the offending or victimization of any type of deviance. Enabled by the LCA approach, the current study was able to move above and beyond the victim-offender matrix and revealed that high-risk "generalist" offending-victimization overlap was rare, but "specialist" (i.e., concentrating on a select few types of online deviance) overlap with a tendency toward either offending or victimization was common. These empirical divergences from the literature also highlight the need for careful consideration of cross-cultural generalizability in this line of inquiry: online

victim-offender overlap patterns may differ from society to society, and more investigations into the developing world are warranted.

The lifestyle-victimization prediction by LET was strongly supported in the current study, echoing previous research (Choi et al., 2017; Holt & Bossler, 2008; Lin et al., 2023; Nodeland, 2020; Partin et al., 2022). Delinquent peer association, offline delinquency, and online information disclosure were particularly strong predictors of high-risk multimodal offending victimization overlap. Moreover, offline delinquent peers played a more significant role than online delinquent peers in predicting high-risk multimodal offending-victimization overlap as well as high-risk multimodal victimization only. This finding confirms yet simultaneously complicates findings from previous research (Dearden & Parti, 2021; McCuddy, 2021; Weulen Kranenbarg et al., 2019; Zhou et al., 2024), which found a more significant influence from offline peers. Findings from the current study suggest that both online and offline peers could be influential for different groups of individuals characterized by differential risks of offending and victimization.

Apart from deviant lifestyle, which exhibited the strongest effect size, impulsivity, social bonds, and being male were also found to be salient predictors of online offending-victimization overlap. Across the board, impulsivity remained a significant predictor of all overlap patterns of online offending and victimization, congruent with findings from previous research (Bossler & Holt, 2010; Burden, 2023; Kerstens & Jansen, 2016; Lin et al., 2023; Mesch et al., 2018; Partin et al., 2022; Reyns et al., 2019; Van Wilsem, 2013; Weulen Kranenbarg et al., 2019). In contrast, parental and school bonds showed heterogeneous effects in predicting different latent classes. Overall, we found that school bonds had a more consistent impact in predicting different overlap patterns than parental bonds. Individuals who were primarily online victims were associated with weak school bonds, suggesting that they may be experiencing difficulty in school and choosing the Internet as an escape, even though their Internet exposure seemed to have also made them vulnerable to online victimization. Those who offended across multiple types of deviance and experienced a relatively low incidence of victimization also reported weak school bonds, indicating a potential alienation from school life for this group as well. However, for higher-risk "generalist" victim-offenders, parental bond was also a significant predictor in addition to school bond. This finding is partially consistent with those reported by Kerstens and Jansen (2016) that victim-offenders showed weaker parental bonds but not peer or school bonds.

Regarding sociodemographic factors, we found that compared to male students, female students were at a much lower risk of offending or victimization, but the effect is especially large when it comes to multimodal

offending and overlap. Although the inconsistent effects of gender in online offending-victimization overlap have been documented (Burden, 2023; Kerstens & Jansen, 2016; Nodeland, 2020; Parti et al., 2022; Weulen Kranenbarg et al., 2019), among those that identified significant gender differences (Burden, 2023; Kerstens & Jansen, 2016; Parti et al., 2022), males were found more likely to be online victim-offenders than females. Our study provides the very first evidence of a gender effect in predicting the differential risks of online offending-victimization overlap in the Chinese context.

In contrast, the present study only observed limited applicability of routine activity theory in explaining online offending-victimization overlap. Although we intentionally included multiple routine activity indicators, the results suggested that only a few variables showed significant effects in predicting overlap across all examined models, and those effects were ambiguous. For example, compared with the baseline group, individuals in the high-risk multimodal offending with minimal victimization group were more likely to report high social media guardianship. This finding reflects the guardianship tenet of routine activity theory. However, individuals in the high-risk multimodal overlap group *also* reported high social media guardianship, obscuring the influence of guardianship on overlap risk. Furthermore, both measures of online exposure (time spent online and the number of social media accounts) were theoretically assumed and empirically identified as a positive associate of online victimization (Reyns et al., 2011; Pratt et al., 2010), but we found the latter had the opposite effect in the context of online offending-victimization overlap (when comparing LC4 with LC1).

The findings from this study carry several policy implications. First, the LCA approach taken by the current study revealed that offending and victimization risks are heterogeneous across online deviance types. Online harassment and sexual harassment seem to be the most prevalent type of offense among Chinese youth in the current sample, followed by violent threats and abuse. Meanwhile, having online accounts stolen, having been defrauded, and having been bullied constituted the most common types of online victimization. These findings suggest that online interpersonal conflict and inappropriate behaviors, along with instrumental victimization such as fraud and theft, are of significant concern among Chinese youth and should be prioritized in prevention and intervention efforts. Second, prevention efforts should aim to disrupt lifestyle risk factors such as online delinquent peer association and online disclosure of personal information. This can be done by providing more effective regulations and targeted, accessible, and restorative education on cybersecurity to Chinese youth (Robalo & Abdul Rahim, 2023). Finally, enhancing parental and school bonds is critical to reducing online offending and victimization, especially for those who are most at risk. Programmatically,

this means providing teachers with resources such as educational material on cybersecurity and online deviance, developing a "triage" system to identify the most at-risk groups of youth and provide customized professional and restorative support to strengthen their school and family bonds, as well as coordinating multi-agency prevention and intervention (e.g., parents, schools, and social service providers) targeting at-risk youth's school and family life.

Concededly, there are several limitations to the current study. First, the sample from this study was limited to Chinese youth from one educational institution. Caution is advised, therefore, when generalizing the findings from the current study to the population of all Chinese youth. Future studies can test the generalizability of the findings from the present research by incorporating more diverse samples, such as youth from other localities in China. Secondly, the multivariate analyses did not exhaust all possible criminogenic and victimogenic factors. Future research adopting more sophisticated operations and complete theoretical constructs is strongly encouraged. For instance, while the measures for online delinquent peer association closely matched those used for the respondents' online offending and victimization, the measures for offline delinquency did not reflect the offline offending measures adopted in the current study. Instead, they only focused on lifestyle deviance, such as drinking, smoking, and partying. Future research should supplement measures of offline delinquency with antisocial behaviors, such as fighting, shoplifting, or bullying others. Thirdly, the current study also did not exhaust all online deviance types. Future research should consider a broader scope of online deviant behaviors (such as digital piracy) and victimization to examine if the findings from the current study also hold for other types of online deviance. Finally, many variables in the present study, such as delinquent peer association, were measured by self-reported responses, which may be affected by the respondents' subjective bias (Rosenman et al., 2011). Future studies may consider combining self-reported and peer-reported/parent-reported responses to minimize the biases caused by the participants' subjectivity.

In conclusion, by implementing LCA and posterior multinomial logistic regression analysis, this study not only provides insights into the differential risks of online victim-offender overlap across online deviance types and accentuates the importance of methodological diversity in this line of inquiry, but it also offers evidence concerning the applicability of multiple criminological theories in predicting overlap in the Chinese context. In particular, we identified five latent classes of youth with differential risks and patterns of online victim-offender overlap, indicating the strength of LCA in detecting the nuanced patterns of overlap. Findings from the posterior regression analysis suggest that LET exhibits greater explanatory power in overlap risks

than other examined criminogenic and victimogenic factors (e.g., self-control, social bonds, and routine online activities).

## Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

## Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: The research is supported by the "Fundamental Research Funds for the Central Universities" (Grant Number: 24CXTD02).

## ORCID iDs

Kai Lin https://orcid.org/0000-0003-3966-0009
You Zhou https://orcid.org/0000-0002-9255-5403

## References

Akers, R. L., & Jennings, W. G. (2019). The social learning theory of crime and deviance. In: M. Krohn, N. Hendrix, G. Penly Hall, & A. Lizotte (Eds), *Handbook on crime and deviance. Handbooks of sociology and social research*. Springer, Cham. https://doi.org/10.1007/978-3-030-20779-3_6

Back, S., Soor, S., & LaPrade, J. (2018). Juvenile hackers: An empirical test of self-control theory and social bonding theory. *International Journal of Cybersecurity Intelligence & Cybercrime*, *1*(1), 40–55.

Bossler, A. M., & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice*, *38*, 227–236.

Brislin, R. W. (1970). Back-translation for cross-cultural research. *Journal of Cross-Cultural Psychology*, *1*(3), 185–216.

Burden, M. (2023). The cybercrime victim-offender overlap: evaluating predictors for victims, offenders, victim-offenders, and those who are neither. *Victims & Offenders*, 1–19. https://doi.org/10.1080/15564886.2022.2159598

Burt, C. H. (2020). Self-control and crime: beyond Gottfredson & Hirschi's theory. *Annual Review of Criminology*, *3*, 43–73.

Chen, J. (2021). "You are in trouble!": A discursive psychological analysis of threatening language in Chinese cellphone fraud interactions. *International Journal for the Semiotics of Law-Revue internationale de Sémiotique juridique*, *34*(4), 1065–1092.

China Academy of Information and Communications Technology (CAICT). (2020). 新形势下电信网络诈骗治理研究报告 [Research report on telecom/cyber fraud intervention in evolving contexts]). CAICT. Retrieved March 25, 2023, from http://www.caict.ac.cn/kxyj/qwfb/ztbg/202012/P020201218393889946295.pdf

Choi, K. S., & Lee, J. R. (2017). Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory. *Computers in Human Behavior*, *73*, 394–402.

Choi, K. S., Lee, S. S., & Lee, J. R. (2017). Mobile phone technology and online sexual harassment among juveniles in South Korea: Effects of self-control and social learning. *International Journal of Cyber Criminology*, *11*(1), 110–127.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588–608.

Cohen, L. E., Kluegel, J. R., & Land, K. C. (1981). Social inequality and predatory criminal victimization: An exposition and test of a formal theory. *American Sociological Review*, *46*(5), 505–524.

Cramer-Flood, E. (2021). *Over 45% of China's digital shoppers will buy via livestream in 2023*. Emarketer. Retrieved March 25, 2022, from https://www.emarketer.com/content/over-45-of-china-s-digital-shoppers-will-buy-via-livestream-2023

Dearden, T. E., & Parti, K. (2021). Cybercrime, differential association, and self-control: knowledge transmission through online social learning. *American Journal of Criminal Justice*, *46*(6), 935–955.

Engström, A. (2021). Conceptualizing lifestyle and routine activities in the early 21st century: A systematic review of self-report measures in studies on direct-contact offenses in young populations. *Crime & Delinquency*, *67*(5), 737–782.

European Commission, Directorate-General for Migration and Home Affairs. (2020). *Europeans' attitudes towards cyber security*, European Commission. https://data.europa.eu/doi/10.2837/672023

Ferguson, L., Elliott, M., & Kim, S. (2023). Examining the connection between missing persons and victimization: An application of lifestyle exposure Theory. *Crime & Delinquency*, *69*(3), 656–681.

Gottfredson, M. R. (1981). On the etiology of victimization. *Journal of Criminal Law and Criminology*, *72*(2), 714–726.

Gottfredson, M.R., & Hirschi, T. (1990). *A general theory of crime*. Standford University Press.

Gottfredson, M. R, & Grande-Bretagne. (1984). *Victims of crime: The dimensions of risk* (Vol. 81). H.M. Stationery Office.

Gunter, W. D. (2008). Piracy on the high speeds: A test of social learning theory on digital piracy among college students. *International Journal of Criminal Justice Sciences*, *3*, 54–68.

Hagenaars, J. A., & McCutcheon, A. L. (2002). *Applied latent class analysis*. Cambridge University Press.

Harrell, E. (2024). *Data breach notifications and identity theft, 2021*. The U.S. Bureau of Justice Statistics. Retrieved May 30, 2024, from https://bjs.ojp.gov/data-breach-notifications-and-identity-theft-2021

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization*. Ballinger.

Higgins, G. E., & Makin, D. A. (2004). Self-control, deviant peers, and software piracy. *Psychological Reports*, *95*(3), 921–931.

Hirschi, T. (1969). *Causes of delinquency*. University of California Press.

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, *30*(1), 1–25.

Holt, T. J., Bossler, A. M., & May, D. C. (2012). Low self-control, deviant peer associations, and juvenile cyberdeviance. *American Journal of Criminal Justice*, *37*, 378–395.

Internet Crime Complaint Center (IC3). (2022). *Internet crime report 2021*. Federal Bureau of Investigation. Retrieved March 25, 2023, from https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

James, G., Witten, D., Hastie, T., & Tibshirani, R. (Eds.). (2013). *An introduction to statistical learning: with applications in R*. Springer.

Jin, X., Zhang, K., Twayigira, M., Gao, X., Xu, H., Huang, C., & Shen, Y. (2023). Cyberbullying among college students in a Chinese population: Prevalence and associated clinical correlates. *Frontiers in Public Health*, *11*, 1100069.

Kerstens, J., & Jansen, J. (2016). The victim–perpetrator overlap in financial cybercrime: Evidence and reflection on the overlap of youth's online victimization and perpetration. *Deviant Behavior*, *37*(5), 585–600.

Kraft, E., & Wang, J. (2010). An exploratory study of the cyberbullying and cyberstalking experiences and factors related to victimization of students at a public liberal arts college. *International Journal of Technoethics*, *1*(4), 74–91.

Lee, C. S. (2021). Online fraud victimization in China: A case study of Baidu Tieba. *Victims & Offenders*, *16*(3), 343–362.

Lenhart, A., Ybarra, M., & Price-Feeney, M. (2016). *Nonconsensual image sharing: One in 25 Americans has been a victim of "revenge porn."* Data & Society Research Institute. Retrieved May 30, 2024, from https://apo.org.au/sites/default/files/resource-files/2016-12/apo-nid266206.pdf

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263–280.

Li, C. K., Holt, T. J., Bossler, A. M., & May, D. C. (2016). Examining the mediating effects of social learning on the low self-control—Cyberbullying relationship in a youth sample. *Deviant Behavior*, *37*(2), 126–138.

Lin, K., Wu, Y., Sun, I. Y., & Qu, J. (2023). Telecommunication and cyber fraud victimization among Chinese college students: An application of routine activity theory. *Criminology & Criminal Justice*, 17488958221146144. https://doi.org/10.1177/17488958221146144

McCuddy, T. (2021). Peer delinquency among digital natives: The cyber context as a source of peer influence. *Journal of Research in Crime and Delinquency*, *58*(3), 306–342.

Mesch, G. S., & Dodel, M. (2018). Low self-control, information disclosure, and the risk of online fraud. *American Behavioral Scientist*, *62*(10), 1356–1371.

Nodeland, B. (2020). The effects of self-control on the cyber victim-offender overlap. *International Journal of Cybersecurity Intelligence & Cybercrime*, *3*(2), 4–24.

Nofziger, S. (2009). Deviant lifestyles and violent victimization at school. *Journal of Interpersonal Violence*, *24*(9), 1494–1517.

Parti, K., Dearden, T. E., & Hawdon, J. (2022). Understanding the overlap of online offending and victimization: using cluster analysis to examine group differences. *Victims & Offenders*, *17*(5), 712-734.

Partin, R. D., Meldrum, R. C., Lehmann, P. S., Back, S., & Trucco, E. M. (2022). Low self-control and cybercrime victimization: An examination of indirect effects through risky online behavior. *Crime & Delinquency*, *68*(13–14), 2476–502.

Pratt, T. C., & Cullen, F. T. (2000). The empirical status of Gottfredson and Hirschi's general theory of crime: A meta-analysis. *Criminology*, *38*(3), 931–964.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, *47*(3), 267–296.

Pratt, T. C., & Turanovic, J. J. (2016). Lifestyle and routine activity theories revisited: The importance of "risk" to the study of victimization. *Victims & Offenders*, *11*(3), 335–354.

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior*, *38*(11), 1149–1169.

Reyns, B. W. (2015). A routine activity perspective on online victimization: Results from the Canadian General Social Survey. *Journal of Financial Crime*, *22*(4), 396–411.

Reyns, B. W., Fisher, B. S., Bossler, A. M., & Holt, T. J. (2019). Opportunity and self-control: Do they predict multiple forms of online victimization? *American Journal of Criminal Justice*, *44*, 63–82.

Robalo, T. L. A., & Abdul Rahim, R. B. B. (2023). Cyber victimisation, restorative justice and victim-offender panels. *Asian Journal of Criminology*, *18*(1), 61–74.

Rosenman, R., Tennekoon, V., & Hill, L. G. (2011). Measuring bias in self-reported data. *International Journal of Behavioral and Healthcare Research*, *2*(4), 320–332.

Sampson, R. J., & Laub, J. H. (1990). Crime and deviance over the life course: The salience of adult social bonds. *American Sociological Review*, *55*(5), 609–627.

Sampson, R. J., & Lauritsen, J. L. (1990). Deviant lifestyles, proximity to crime, and the offender-victim link in personal violence. *Journal of Research in Crime and Delinquency*, *27*(2), 110–139.

Schenk, A. M., & Fremouw, W. J. (2012). Prevalence, psychological impact, and coping of cyberbully victims among college students. *Journal of School Violence*, *11*(1), 21–37.

Stack, S., Wasserman, I., & Kern, R. (2004). Adult social bonds and use of internet pornography. *Social Science Quarterly*, *85*(1), 75–88.

Sutherland, E. H. (1947). *Principles of criminology* (4th ed.). J. B. Lippincott.

Van Wilsem, J. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology*, *8*(2), 115–127.

Van Wilsem, J. (2013). 'Bought it, but never got it' assessing risk factors for online consumer fraud victimization. *European Sociological Review*, *29*(2), 168–178.

Wang, L. (2021). 反诈专门立法，全面打响一场与电信网络诈骗的“攻防战 [Legislating against fraud: a “battle” against telecom/cyber fraud]. CCTV. Retrieved March 23, 2023, from https://news.cctv.com/2021/10/27/ARTINkh8kaKvZap9Igz5tSR8211027.shtml#:~:%20text=央视网消息（记者王莉莉，群众损失353.7亿元）

Weller, B. E., Bowen, N. K., & Faubert, S. J. (2020). Latent class analysis: A guide to best practice. *Journal of Black Psychology*, *46*(4), 287–311.

Weulen Kranenbarg, M., Holt, T. J., & Van Gelder, J. L. (2019). Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap. *Deviant Behavior*, *40*(1), 40–55.

Xu, B., Zhou, Y., & Chang, Y. C. L. (2021).青少年网络越轨行为的发生过程及原理——基于自我控制理论和差别交往理论的视角 [The causes of online delinquencies among Chinese adolescents—The perspectives from self-control theory and differential association theory], *China Youth Social Sciences*, *40*(3), 79–87. https://doi.org/10.16034/j.cnki.10-1318/c.2021.03.010

Xu, Y. (2022). *Research on offenders' decision-making of new cyber fraud crime*. East China University of Political Science and Law. [Unpublished dissertation].

Xu, Y., & Xu, T. (2021). Research on the characteristics and countermeasures of cross-border telecom-network fraud: Based on 18 typical cases. *Issues on Juvenile Crime and Delinquency*, *4*, 88–103.

Zhou, Y., Liu, W., Lee, C., Xu, B., & Sun, I. (2024). Traditional social learning predicts cyber deviance? Exploring the offending versatility thesis in social learning theory. *Behavioral Sciences & the Law*, 1–18. https://doi.org/10.1002/bsl.2664

Zhuang, S. (2020). 谁在直播电商平台“买买买 [Who are buying on livestream e-commerce platforms?]. Tencent Cloud. Retrieved March 25, 2022, from https://cloud.tencent.com/developer/article/1628777

## Author Biographies

**Kai Lin** is a Lecturer in the School of International Studies and Education at the University of Technology Sydney in Australia. His research interests include the etiology of interpersonal violence, international and comparative criminology, policing, queer criminology, and cybercrime. His publications have appeared in journals such as *Crime & Delinquency*, *Criminology & Criminal Justice*, *Journal of School Violence*, *Journal of Interpersonal Violence*, *Policing & Society*, etc.

**You Zhou** is an Assistant Lecturer and a doctoral candidate in the School of Social Sciences at Monash University. His research interests include cybercrime, cyber fraud, policing (cyber fraud), youth violence, criminological theories, and mixed methods. His recent works have appeared in *Sexual Abuse*, *Victims & Offenders*, *Behavioral Sciences & the Law*, and *Journal of Community Psychology.*

**Boyang Xu** is an Assistant Professor in the School of Criminal Justice at China University of Political Science and Law. His research field includes cyber deviance, juvenile delinquency, social psychology, social mentality, police trust, etc. His

research has been published in such journals as *Sexual Abuse*, *Behavioral Sciences & the Law*, *Youth Studies (CSSCI)*, and *Journal of Psychological Science (CSSCI).*

**Lennon Y.C. Chang** is an Associate Professor in the Centre for Cyber Resilience and Trust and the School of Information Technology at Deakin University. He is interested in researching crime and governance of cyberspace, cyber terrorism, and cyber warfare, particularly in Asia-Pacific. His research has been published in such journals as *Regulation & Governance*, *Journal of Criminology*, *Asian Journal of Criminology*, *Police Practice & Research*, and *Computers & Security*.