



## Victims & Offenders

An International Journal of Evidence-based Research, Policy, and Practice

ISSN: (Print) (Online) Journal homepage: <https://www.tandfonline.com/loi/uvao20>

# Online Fraud Victimization in China: A Case Study of Baidu Tieba

Claire Seungeun Lee

To cite this article: Claire Seungeun Lee (2021) Online Fraud Victimization in China: A Case Study of Baidu Tieba, *Victims & Offenders*, 16:3, 343-362, DOI: [10.1080/15564886.2020.1838372](https://doi.org/10.1080/15564886.2020.1838372)

To link to this article: <https://doi.org/10.1080/15564886.2020.1838372>



Published online: 16 Feb 2021.



Submit your article to this journal [↗](#)



Article views: 76




View related articles [↗](#)



View Crossmark data [↗](#)



# Online Fraud Victimization in China: A Case Study of Baidu Tieba

Claire Seungeun Lee 

School of Criminology and Justice Studies, University of Massachusetts Lowell, Lowell, Massachusetts, USA

## ABSTRACT

When it comes to online populations and markets, China has some of the largest in the world. As a result, Chinese cybercriminals have more opportunities to target and access victims. While extant research in Western countries has examined online fraud victimization and offenses in virtual communities, a relatively small body of research on these phenomena has been conducted in non-Western societies. This study attempts to address this gap by analyzing online fraud victimization in Chinese online communities. Routine activity theory is applied to understand the patterns and dynamics of victimization. Data were collected from Baidu Tieba (a Chinese version of Craigslist), a prominent Chinese online platform for reporting victimization. This study highlights the range of services, types, and methods along which victimization occurs. The results, which reflect China's rapid pace of technological development, show that different types of fraud are perpetrated online and that victimization methods are associated with particular types of media. This study also identifies implications for China and other countries where similar crimes and instances in cyberspace occur.

## KEYWORDS

Online fraud; computer crime; victimization; social media; Baidu Tieba; China

## Introduction

The Internet creates countless venues and opportunities for crime and deviance in cyberspace. Online fraud is not only documented as one of the most frequently occurring crimes on the Internet, but it is also well known as one of the varieties of crime in which non-reporting victimization often occurs (Cross, 2016). Online communities serve as a platform to enable an understanding of victimization. In other words, victims share information, maintain solidarity, and often prepare for further collective actions together in virtual communities. Therefore, studying an online platform enables clear access to observe instances of victimization.

China has the largest connected population in the world. In March 2020, desktop and mobile Internet users in China numbered 904 million and 897 million, respectively (China Internet Network Information Center [CNNIC], 2020). As a platform similar to Craigslist, Baidu Tieba, which is lesser known in other parts of the world, is one of China's three largest social media platforms along with WeChat and Weibo – the Chinese counterparts to WhatsApp and Twitter. Its primary function is to facilitate access to interest groups online (Liu & Lu, 2018; Stockmann & Luo, 2017). Like other social media networks, WeChat and

Weibo have become particularly popular outlets for and facilitators of cybercrime in recent years (Gao & Zhang, 2015). In contrast, Baidu Tieba has become established as a platform on which victims can share their experiences of being victimized and warn other potential victims.

Previous studies of China's emergent Internet focus mostly on online communities, online spaces and society (Herold & Marolt, 2011; Marolt & Herold, 2015), online parody (Meng, 2011), contentious politics and online activism (Sullivan & Xie, 2009; Yang, 2011), and censorship (King et al., 2013, 2014; Liang & Lu, 2010), as well as Internet sovereignty (Jiang, 2010). Despite the Chinese Internet and cyberspace being an accumulative presence in the existing literature, any academic focus on crime and deviance and victimization in China is scarce, in both English and Chinese. Although online communities and platforms generally garner attention as sources of and venues for research in communication, sociology, and criminology, much of this line of inquiry explores U.S.-centered or English-language platforms, such as the original Craigslist (e.g., Frederick & Perrone, 2014; Garg & Nilizadeh, 2013; Grov, 2012; Lair & Andrews, 2018; Lair et al., 2016; Moskowitz & Seal, 2010; Oliveri, 2010; Park et al., 2014; Robinson & Vidal-Ortiz, 2013; Rosenbaum et al., 2013; Tofighi et al., 2016). Not only are English-language studies on China's cybercrime scarce (Liang & Lu, 2010, p. 111), but the intentional exploration of online web forums to understand Chinese cybercrime dynamics is also limited, unlike cases in other countries (Holt et al., 2016). More critically, from a theoretical standpoint, cybercrime from a cyber-victimization perspective is a well-established field of research in the United States, whereas cybercrime is still an understudied area in China; only recently and slowly has attention to it increased. In particular, research that draws from social media is even more limited: only a few studies published in Chinese discuss the various types of WeChat fraud (Xu, 2016; Yuan & Ye, 2016). Likewise, cybercrime, having emerged relatively recently compared with other crime typologies, has not yet become a major research area in Chinese criminology or related fields.

This study extends the extant literature by examining a Chinese online platform as an arena for reporting online fraud victimization, looking in particular at victims' behavioral traits that may poise them as targets (i.e., patterns of online fraud in China) and inside the patterns of victimization reporting (e.g., frequently described victimization methods and media types). The present study explores whether a type of media (i.e., online presence) leads to divergent patterns of online fraud victimization by laying a foundation of routine activities theory. This study shows that Baidu Tieba is used in China as a platform both to report online fraud victimization and to mediate online fraud. Analyzing these contingencies, the Chinese context of cyberspace, social media, and online fraud enables the study to make a contribution not only to broader online fraud literature but also to offset the Western bias of that literature. In doing so, this paper enhances our understanding of the online fraud literature that is cultivated predominantly from Western contexts by investigating online fraud in relation to the social media types and victimization methods in China, one of the world's largest markets of Internet users and, arguably, cybercrime as well. Due to China's unique background regarding online fraud, cyberspace, social media, and the historical, legal, and institutional contexts in relation to these landscapes, understanding online fraud victimization in the Chinese setting also highlights the lack of research with a non-Western focus. Finally, this study has political and practical implications. Since cyberspace is boundaryless, and access to China's Internet users and online platforms

offer a unique opportunity for cybercriminals to utilize such conditions, an exploration of understudied Chinese cybercrime markets may identify new avenues for other countries to review their cybercrime prevention policies.

This paper is organized as follows: The first section reviews the conceptual and empirical background of online fraud and its extant literature. Next, the paper presents the relevant data, research methodology, and research findings. The final section summarizes the conclusions of the research and identifies practical and policy implications. This study also addresses implications of online fraud victimization for wider audiences.

## Literature review

### *Online fraud victimization*

The term “online fraud” refers to “the experience of an individual who has responded through the use of the internet to a dishonest invitation, request, notification or offer by providing personal information or money which has led to the suffering of a financial or non-financial loss of some kind” (Cross, 2016; Cross et al., 2014, p. 1). Online fraud intends to exploit people by using online platforms to gain access to them (Buchanan & Whitty, 2014). Online fraudsters utilize a wide range of methods to infringe upon victims’ personal information and typically lure and persuade them to do certain things that will result in financial damages (Pratt et al., 2010; Reyns, 2013; Zahedi et al., 2015). Current scholarship on online fraud tends to focus largely on archetypes of these crimes, including “‘get rich quick frauds’ (e.g., the advance-fee fraud, lottery frauds, fake prize frauds)” (Buchanan & Whitty, 2014, p. 263), online dating romance scams (Buchanan & Whitty, 2014; Rege, 2009; Whitty & Buchanan, 2012), online consumer fraud victimization (Van Wilsem, 2013), online auction fraud (Conradt, 2012; Dolan, 2004), and phishing (Lee, 2020; Leukfeldt, 2014). Other scholars have studied the psychology and trauma experienced by elderly fraud victims (Cross, 2016, 2017; Mears et al., 2016), prevention strategies and approaches to online fraud (Cross, 2016; Cross & Kelly, 2016), reporting fraud (Cross, 2016, 2018), refund fraud (nonpayment fraud), and return fraud (non-delivery fraud) (Maimon et al., 2019).

While scholars acknowledge that online fraud is not a particularly new phenomenon but rather one augmented by the evolution of technology (Yar, 2013), a few issues exist within the growing body of literature. First, what is still left relatively unknown are common features among fraud victims (Buchanan & Whitty, 2014); specifically, little research has focused on particular technologies, online platforms, media, and tactics that feature in victimization via online fraud. Second, the existing literature is geographically focused predominantly on Western countries. Given China’s lucrative and vibrant Internet environment, it is surprising to see that research emphasis exists only on China’s online services (banking, e-commerce, shopping), particularly related to positive growth, economic perspectives and consumer satisfaction (Laforet & Li, 2005; D. Li et al., 2008; Lin & Li, 2005; Yang et al., 2009; Yoon, 2010), ignoring crime and deviance. In fact, the body of literature on cybercrimes in China is relatively limited (exceptions include Chang, 2012; Liang & Lu, 2010; Lu et al., 2010). Among the studies of Chinese cybercrime that do exist, very few have explored fraud. Instead, the existing research covers, for example, online shopping from the perspective of consumer risk (Ye, 2004), financial fraud in online markets and e-commerce (Guo et al., 2018; Zhang et al., 2013), risk assessment of financial frauds and fraud cases on

the Chinese online shopping site Alibaba (Chen et al., 2015; Song et al., 2014; Zhang et al., 2013), and corporate fraud in China (Chen et al., 2016; Conyon & He, 2016).

### ***Online communities as venues for online fraud: Baidu Tieba***

A wide range of topics and activities are present on Craigslist, one of the most widespread virtual spaces in the United States since its launch in 1995, and it has been studied as a significant site for social and cultural activities (Hanson & Hawley, 2011; Kroft & Pope, 2014; Lair et al., 2016; Oliveri, 2010; Robinson & Vidal-Ortiz, 2013). Its innovative and far-reaching characteristics have attracted researchers who dive into its details as points for data analysis. Specific themes have emerged from this literature, including the notion of virtual communities as gated communities (Schackman, 2010), and research on housing (Hanson & Hawley, 2011; Oliveri, 2010), nanny advertisements (Lair & Andrews, 2018; Lair et al., 2016), same-sex partner matching, romantic relations, and other consequences (Frederick & Perrone, 2014; Moskowitz & Seal, 2010; Robinson & Vidal-Ortiz, 2013; Rosenbaum et al., 2013), HIV (Groß, 2012), substance use (Tofghi et al., 2016), and legal matters (Radbod, 2010). Despite the extensive existing research on Craigslist, there are only a few studies of the platform as a venue and source for understanding victimization and criminal cases (e.g., online fraud victimization [Garg & Nilizadeh, 2013; Park et al., 2014]. Garg and Nilizadeh (2013) used the 30 largest metropolitan areas represented on Craigslist to examine automobile fraud using a macro-level approach and OLS regression analyses, finding that the characteristics of cities (e.g., racial homogeneity, per capita income) are associated with the exposure of fraud. Park et al. (2014) explored cases of advance-fee fraud – also known as Nigerian fraud – and characteristics of the fraudsters by using magnetic honeypot advertisements. Their findings showed that most fraudsters are located in Nigeria and that the accounts of 10 groups were highly involved in attempts to defraud others.

Baidu Tieba, a platform similar to Craigslist that operates in China, was launched in 2003. Like its U.S. counterpart, Baidu Tieba is a virtual community featuring classified advertisements that offer a single place for sharing information, goods, and services in multiple cities without the need to switch between websites. Baidu Tieba is more of an interest-based online community than a location-based one. One might assume that researchers would be drawn by the popularity and potential value of Baidu Tieba to look deeply at the site as both an online service provider and a community in China; however, given that it has already existed for more than 15 years but garnered little scholastic notice, this does not appear to be the case. Scholars have paid only limited attention to this platform, focusing on public opinion and fandom (L. Li et al., 2013; Stockmann & Luo, 2017), word-of-mouth effects on films (Godes & Mayzlin, 2004; Liu, 2006), and HIV-positive users (Liu & Lu, 2018). Also, Wu et al. (2014) have studied Baidu Tieba web forums in comparison with platforms Delicious and Flickr, to identify networks and dynamics of clickstreams. Perhaps a level of inaccessibility in terms of language barriers and censorship has prevented the Chinese Internet from becoming an attractive site for the study of criminal activities.

A few Craigslist studies show that cases of victimization through advertisements and threads posted on the site can provide important insights into cyberspace (e.g., Lair & Andrews, 2018; Lair et al., 2016; Park et al., 2014; Radbod, 2010). In a similar vein, some scholars point to Baidu Tieba as a venue for Chinese cybercrime and hacking (Fang et al., 2016; Yip, 2011). However, less is known about victimization on the same platform.

In an attempt to fill the gaps left by previous studies and to collect primary data innovatively in conducting cybercrime research (Bossler & Berenblum, 2019), this study analyzes Baidu Tieba as a venue for discussing and reporting cases of victimization from crimes related to a technology-based device or technological element. The following section describes the data, measures, and methodology used in this analysis.

### ***Routine activity theory as an analytical framework***

The routine activity theory (RAT) explains the frequency of criminal opportunities at the macro-level and the micro-level (Clarke & Felson, 1993). Its main propositions are that crime occurs as a result of the convergence of three elements – a suitable target, a motivated offender, and the lack of capable guardian – in space and time (Cohen & Felson, 1979). The RAT was initially proposed to explain a specific category of crime known as “direct-contact predatory violations” (Cohen & Felson, 1979, p. 589), which consists of crimes that involve direct physical contact during which one party takes or damages the other party or their property (Cohen & Felson, 1979, p. 589). Cohen and Felson (1979) propose that the occurrence of these violations is affected by the spatial and temporal components of community structure, which is composed of human interactions and relationships. The spatial component refers mainly to the physical locations in which the interactions and relationships occur. The temporal components are divided into three aspects: rhythm, tempo, and timing. These aspects of RAT’s temporal components address the regularity and the frequency of crime occurrences and the activities that result from the interactions of that regularity and frequency (Clarke & Felson, 1979).

In the original conception of the RAT, motivated offenders were seen as the least important of the theory’s three elements because the presence of individuals with criminal inclinations is taken for granted (Cohen & Felson, 1979). This is understandable as the purpose of the RAT is to understand the role of community structures and activities in crime patterns and occurrences. The other two components of the framework – a target’s suitability and a lack of guardianship – explain the role of the immediate environment.

In general, at the macro-level, the RAT argues that macro-level crime results from major shifts in routine activities, as criminal acts depend upon the spatial and temporal aspects of routine legal activities (Clarke & Felson, 1979; Felson & Cohen, 1980). The locations of bars and their happy hour schedules, for instance, can predict to an extent the frequency, timing, and sites of assaults with that locale. Cohen and Felson (1979) have also discovered that the frequency of household burglaries during the daytime is directly proportional to the ratio of absent households during that window of time.

At the micro-level, the RAT has been applied to explain the effect of individual behaviors on the nexus of the three crime-conducive elements in physical proximity (Cohen & Felson, 1979). The theory assumes that offenders are intrinsically motivated to commit crime. Therefore, RAT provides a useful framework for exploring victims’ behavioral traits in relation to victimization. First, it addresses victims’ use of the Internet. That is, a researcher can include in their model whether and how frequently a victim uses the Internet; the more often one uses the Internet/social media, the more likely they are to be victimized by online crime writ large resulting from greater exposure to motivated offenders. Second, it explores



the particular types of social media that victims use and how that differentially affects victimization. Third, the relationship between victims and offenders can be used as a proxy for target suitability; that is, one's proximity to another person may be increased depending on the type of relationship they have with that person. Taken together, RAT is a useful framework for examining online fraud victimization in China through the use of Baidu Tieba.

## Data, measures, and methods

### Procedure

The data analyzed in this study were collected and derived from publicly accessible web forums based in China. The web forum Baidu Tieba, on which information, goods, and services are exchanged, was started in 2003. Baidu Tieba caters to interest groups and often features specialized thematic forums that are open to public comment. Figure 1 depicts the homepage of Baidu Tieba and Figure 2 shows a thread titled "Forum on Fraudsters" on the site.

This data was obtained between June and November 2017. To choose which online forums to include in this study, the author specifically searched Baidu Tieba for active *tiebas* (web forums) with a large number of posts and users who are reporting scams and scammers linked to the platform. Then, the author selected one such *tieba*, named *Dapianzi ba* (Forum on Fraudsters), a specialized forum for reporting scams; it included 265 cases between January 2010 and May 2017. In the period before 2010, Baidu Tieba allowed anonymous posting, displaying only the IP address of each poster.

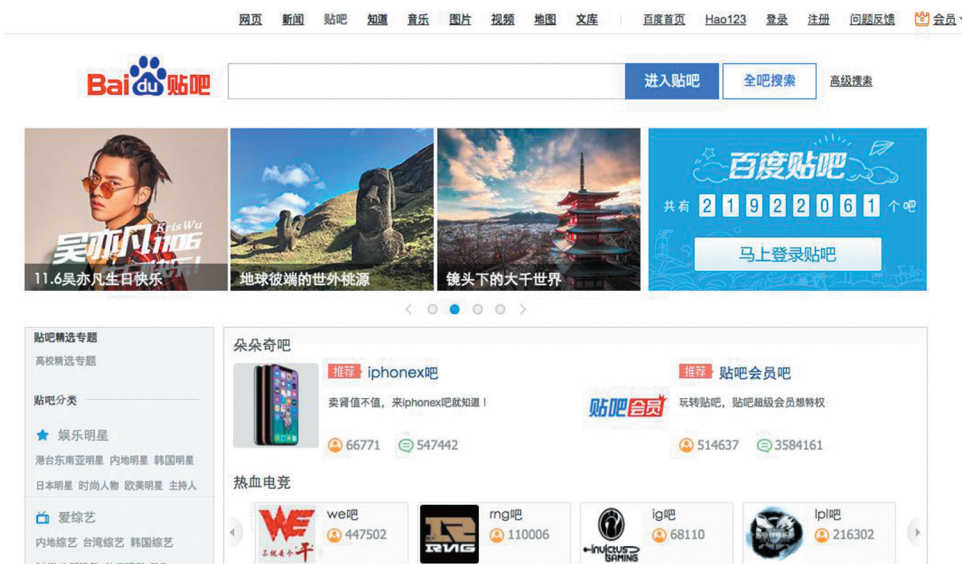
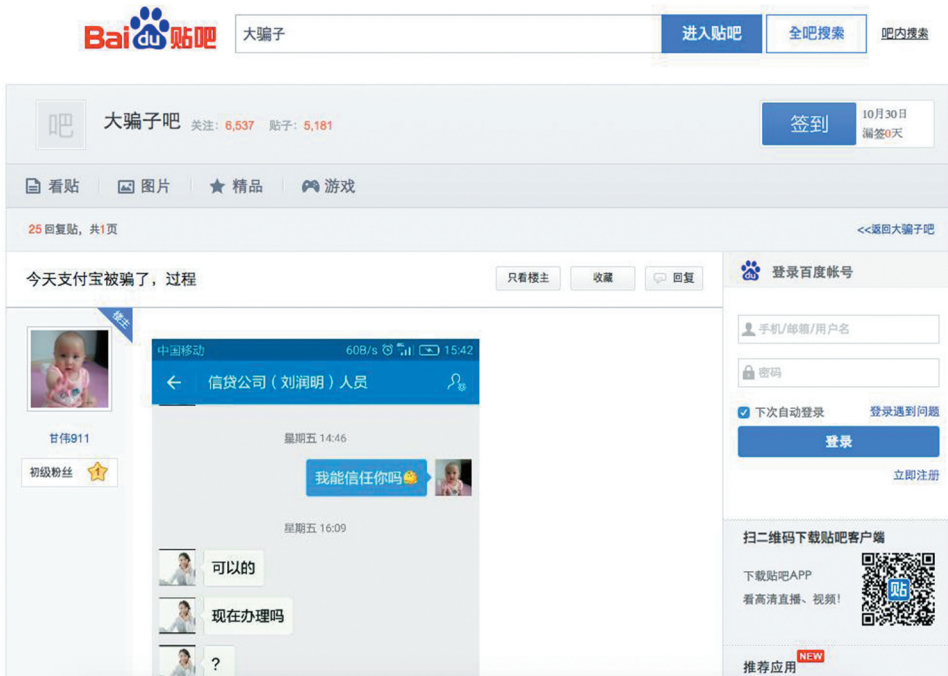


Figure 1. Baidu Tieba.

Source: Baidu Tieba (2018). <https://tieba.baidu.com/index.html>.



**Figure 2.** "Forum on fraudsters" thread on Baidu Tieba.

Source: Forum on Fraudsters (*Dapianzi ba*), 2018. Baidu Tieba. <http://tieba.baidu.com/f/good?kw=%B4%F3%C6%AD%D7%D3&fr=ala0&tpl=5>

The author created a *tieba* database using both manual collection and a crawling method, in part using R. All threads that are publicly accessible were saved as web pages. These threads were initially examined in their original language and then translated into English in later analyses. Two Chinese research assistants reviewed all of the threads carefully and identified terms that were slang, Internet-specific terms, or new words meant to evade any policing by the web platform and the authorities. A dictionary of such terms was prepared for further analysis in order to capture the dynamics of the Chinese Internet.

In addition to identifying important terms for the study, the author coded key themes and keywords for further analysis. The author and the research assistants also coded and cross-checked themes and the information on the forum to create a higher-quality database. The research assistants' coding was then compared with the author's coding using 10% of the sample. Using this method, the inter-coder reliability was found to be 0.79, demonstrating that the codes identified between the coders were reliable (Landis & Koch, 1977).

As a result of such procedures, a total of 265 threads were collected; however, many of the threads either did not contain enough information for analysis or had overlapping information. For example, if a thread mentioned a specific person who was fraudulent but did not include specific information, which occurred frequently, it was deleted due to gaps that made it insufficient for data analysis. In addition, some threads did not pertain to technology-facilitated and online fraud cases and thus were not relevant to this research.

The threads span a seven-year period from 2010 to 2017, but the majority of threads were posted in 2017 (approximately 43.8%). Although the earliest year of posting was 2010,



several threads were about incidents that had occurred prior to the year in which they were posted. For example, users posted about incidents from 2008 in four threads and 2009 in two threads. Ultimately, the data availability of all information in this research resulted in fewer than 300 cases used for analysis.

Because of the characteristics of the Baidu Tieba platform, the data utilized in this research may not reflect all technology-facilitated fraud cases in China as a whole or paint a general picture of such crime scenes. Like other online platforms, Baidu Tieba is largely dominated by younger users who are likely to use the Internet and smartphones in their everyday lives (Liu & Lu, 2018). Furthermore, platforms for exchanging information about fraud cases and victimization are not always open to the public. Baidu Tieba, the platform utilized in this research, is only one of the public places that has not been well explored by criminology researchers – unlike Craigslist, into which recent criminology research has delved in detail. Similar platforms in other countries have also not been researched adequately. Therefore, an investigation of this platform is meaningful. The findings of this study can document an early online venue for sharing information about cybercrime victimization and can also offer a potential direction for future research. By becoming aware of and reading details about previous fraud cases, individuals who may be targeted by similar fraudsters can prevent their potential victimization, and law enforcement agencies can better investigate such cases based on the available online information.

## Methods

This study uses multiple correspondence analysis (MCA) and chi-square tests to understand patterns of online fraud on China's Baidu Tieba. MCA and chi-square tests are useful for studying categorical variables. Furthermore, MCA is powerful in revealing groupings and memberships of variable categories in dimensions (Costa et al., 2013).

## Measures

This research uses MCA to understand victimization by online fraud and, in particular, explore what types of media, methods, and resources are used to commit such crimes as well as identify which types of victimization they intersect with.

## Variables

Table 1 presents the descriptive statistics of relevant variables used in this research.

Variables identified from the database include crime incidents and the methods behind carrying them out. The contents of each variable are as follows: (1) *Type of media*, which includes Alipay, Phone, QQ, Taobao, and WeChat; (2) *Type of victimization method*, including card fraud, fake contacts, phone bill fraud, refund fraud (nonpayment fraud), or return fraud (non-delivery fraud); (3) *Year* indicates year of victimization; and (4) *Victimized money (victimization)* represents the amount of money each victim lost in their victimization (in Chinese Renminbi [¥]). Of all the victims in the dataset ( $N = 265$ ), only 48.3% of the cases ( $N = 128$ ) reported the amount of money involved in their victimization. Although in these cases there is no clear evidence of how much they lost, failure to report the amount of money does not necessarily mean that there was no financial loss. Following this logic, the first category starts from ¥1 and the last category ends with ¥200,000, which was the highest victimized amount in the dataset. With a high degree of

**Table 1.** Descriptive analysis.

<i>Variable</i>	<i>N</i>	<i>%</i>
<i>Year (N=265)</i>		
2008	4	1.5
2009	2	0.8
2010	4	1.5
2011	8	3.0
2012	6	2.3
2013	17	6.4
2014	14	5.3
2015	22	8.3
2016	55	20.8
2017	133	50.2
<i>Type (N=265)</i>		
Alipay	8	3.0
Phone	58	21.9
QQ	151	57.0
Taobao	27	10.2
WeChat	21	7.9
<i>Method (N=265)</i>		
Card fraud	5	1.9
Fake contact	10	3.8
Phone bill fraud	5	1.9
Refund fraud	160	60.4
Return fraud	85	32.1
<i>Victimized money (in ¥) (N=128)</i>		
0–122	32	12.1
123–500	34	12.8
501–3,000	35	13.2
3,001–15,000	14	5.3
15,001–200,000	13	4.9

variability, the amount of victimized money was coded into five categories by using its distribution, for the purpose of statistical testing: ¥1–¥122, ¥123–¥500, ¥501–¥3,000, ¥3,001–¥15,000, and ¥15,001–¥200,000.

### **Analytic strategy**

To explore the patterns and characteristics of online fraud victimization in China, this study uses a mosaic plot – which is a visualization technique arranging the results of a crosstab analysis – and a multiple correspondence analysis (MCA). Mosaic plots, which were developed by Hartigan and Kleiner (1981), are designed to present and explore categorical data in a graphic manner. Each cell of a contingency table is represented by a tile. “The tile’s size is directly proportional to the number of cases in this cell.” To interpret a mosaic plot’s results, the concept of a one-dimensional spineplot, which sheds light on proportions, is useful (Hofmann, 2000).

MCA is used in social sciences as an extended version of correspondence analysis. It systematically explores the patterns of associations between more than two categorical dependent variables (Abdi & Valentin, 2007) and “translates deviations from the independence model in the contingency table into distances” (Blasius & Thiessen, 2001). The general principles of MCA include a proportional relationship between the distance and volume of categories from the center of an axis and their impact on the axis’ shape. On an MCA plot, short distances between data points represent high similarity, whereas long

distances imply dissimilarity (Blasius & Thiessen, 2001, p. 7). In other words, the purpose of an MCA is to locate individuals or items by using similarity-based distance in dimensional spaces. The distances between different variables indicate whether these variables are highly correlated with one another. In criminology, MCA has not yet been widely adopted, but existing research has used this method to explore the internal dynamics of non-organized crime and organized crime in groups such as the mafia (Calderoni et al., 2016) and cyberterrorism (Choi et al., 2018). For non-organized criminal efforts, this analytical plan is also useful in understanding associations of different variables in the research. Thus, it is an effective means of understanding the dynamics of victimization in fraud cases.

Results

Trends in online fraud victimization in China

Before presenting our key research findings, this section briefly describes the context, dataset, and sample characteristics. China’s vast number of Internet users and vast volume of social media and online platforms allow a unique opportunity for cybercriminals looking to utilize such conditions. In Chinese cyberspace, online gambling, pornography, and online fraud are the most frequently observed crimes (China Internet Network Information Center, 2018, 2020) (Internet Crime Reporting Center, 2015, 2016, 2017, 2018, 2019, 2020). The major techniques used to facilitate online fraud crimes in China – information that the Internet Crime Reporting Center no longer makes available to the public – include fake websites; fake trade; establishing friendships with victims through fake contacts on instant messaging service Tencent QQ (commonly known as QQ); selling exam answers or “cheat sheets”; recruitment fraud; and pyramid schemes (Internet Crime Reporting Center, 2016, 2017).

This study observed trends in China’s online fraud victimization in the current data, which is presented in Figure 3. In this dataset, only four cases were documented in 2008. However, the number of cases grew rapidly and a total of 129 cases, or 49% of the whole dataset, were reported in 2017. Fewer than 10% of the cases were reported from 2008 to 2012. With the further penetration of technology and use of Baidu Tieba as a platform, more than 90% of cases were documented from 2013 to 2017.

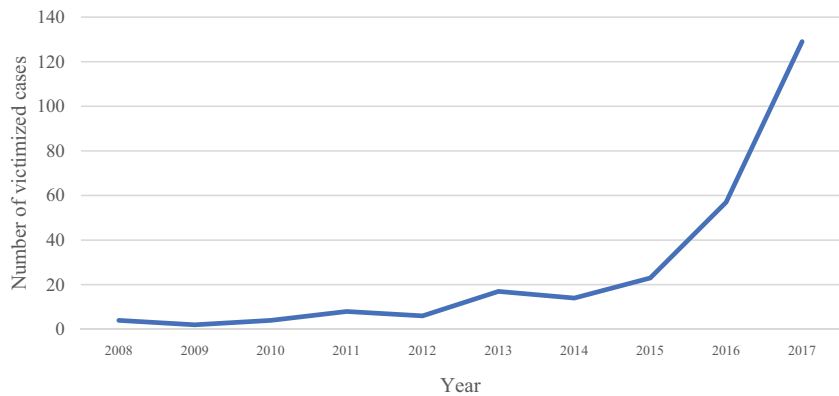


Figure 3. Baidu Tieba’s yearly trends of online fraud victimization.

### Examining the relationship between media types and victimization methods

As described earlier, mosaic plots represent a graphical way of visualizing contingency tables (Hartigan & Kleiner, 1981). The sizes and the positions of each rectangle (or tile) depict the cells in a contingency table (Hofmann, 2008) and the sizes of tiles are proportional to the cell count (Hu, 2004). Figure 4 above shows a mosaic plot of the criminological types and methods, based on the findings of a contingency table. Two types of online fraud show particularly interesting results. Refund fraud (i.e., an online non-delivery fraud) is one type of crime in which customer payments are made without the delivery of goods and services (Internet Crime Reporting Center, 2017; Maimon et al., 2019). Return fraud (i.e., an online nonpayment fraud), on the other hand, is a type of fraud in which goods and services are delivered without payment being made, and then fraudulently requesting money. Only one type of fraud was linked to online payment system Alipay, which is refund fraud (100.00%), while phones were used to commit four different types of fraud; proportionally speaking, the most common were return fraud (61.54%), followed by fake contact (19.22%), card fraud (9.63%), and phone bill fraud (9.61%). Phones were not used in refund fraud victimization. To carry out refund frauds, fraudsters typically advertise an item, product, or service on a classified-advertisement website and contact potential targets via e-mail or phone (Button & Cross, 2017; Maimon et al., 2019). QQ was used predominantly in refund frauds (70.08%), but also in return frauds (29.92%). As one of the largest online shopping and auction websites in China, with an enormous number of users, Taobao was also used predominantly in refund frauds (77.77%) as well as return frauds to a lesser extent (22.23%). WeChat was used predominantly in refund frauds (85.71%), followed by return frauds (14.29%). The resulting chi-square test results were statistically significant ( $\chi^2 = 123.091$ ,  $p < .00$ ).

### Victimization patterns: media types, methods, and years (MCA)

This section describes the kinds of media utilized to contribute to victimization in Chinese cyberspace. MCA methods associate different categorical variables in order to fully comprehend the dynamics of online fraud victimization in China.

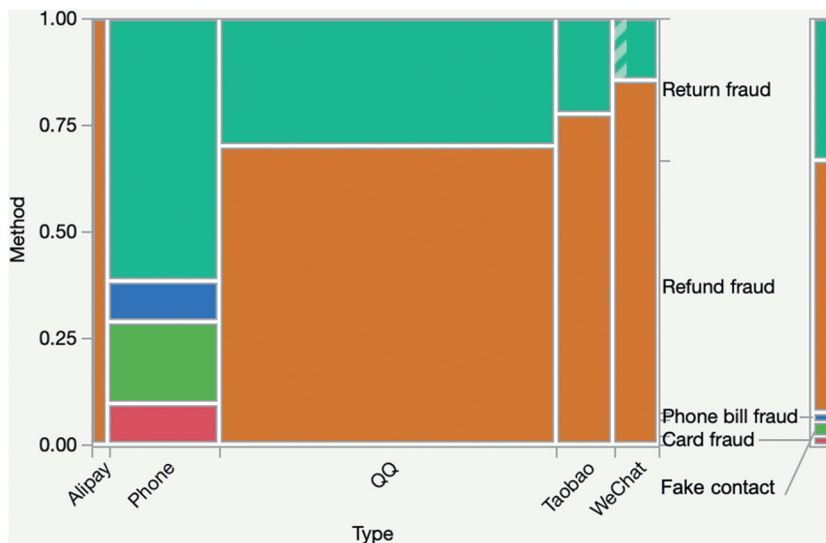


Figure 4. Mosaic plot.

Figure 5 shows the MCA results: i.e., the relationship between types of media, methods of victimization, and years on a joint plot of all these categorical variables along two dimensions. The MCA plot created by juxtaposing media and year had statistically significant results ( $p < .00$ ). The following three clusters were found through MCA. The first cluster (“Phone frauds”) is all about phones (media). Phones were used for and were highly associated with phone bill fraud, fake contacts, and card fraud (in line with the results shown in the mosaic plot). The second cluster (“Social media/Internet with refund frauds”) shows that these types of new media are well clustered with refund fraud. Alipay, an electronic payment service, WeChat, and Taobao are highly associated with refund frauds, particularly in the years 2014, 2016, and 2017. QQ is also associated with refund frauds, but in different years, namely, 2012 and 2015. In the third cluster (“Return frauds”), return

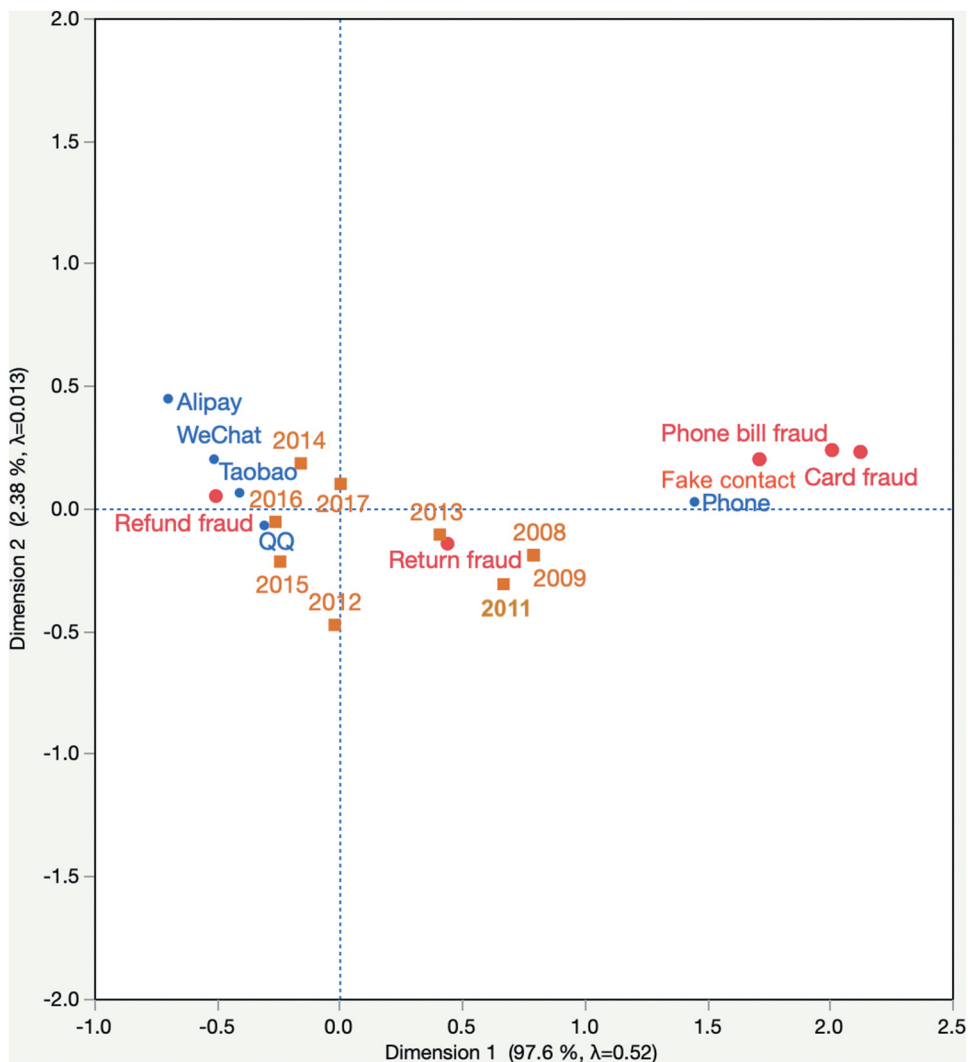


Figure 5. MCA map of method by type.

frauds are associated with 4 years: 2008, 2009, 2011, and 2013. Dimension 1 explains 97.62% of all cases.

QQ, an instant messenger used on phones and PCs, accounts for the majority of cases (57.1%), followed by calls and SMSs via smartphones (21.9%) and Taobao (10.2%), a leading Chinese online auction company; online payment system Alipay and instant messenger WeChat (with WeChat pay) together comprise 7.9% of the dataset. In this dataset, it was found that in cases of wireless and online messengers and online payment systems, phone numbers are used by perpetrators for keeping in touch with victims. This is particularly interesting because it shows that traditional methods of crime were coupled with new and emerging methods, reinforced by technology and the Internet (Button & Cross, 2017).

## Discussion and conclusion

This study examined China's uncharted but rapidly growing cyberspace and how cases of online fraud victimization are being discussed and shared online. Baidu Tieba, a platform much like Craigslist in the United States, was chosen largely because it is a Chinese (and non-English language) community, and located in Asia – particularly China – which is understudied in research on online criminality because of language barriers and censorship.

While extant research in Western countries has examined online fraud victimization and offenses in virtual communities, a relatively small body of research on these phenomena has been conducted in non-Western societies. An emerging body of literature takes this into account and examines online data markets where stolen data was available (Franklin, Paxson, Perrig, & Savage, 2007; Holt, 2012; Holt et al., 2016; Motoyama et al., 2011; Wehinger, 2011), and some cybercrime research uses innovative methods such as analyses of online forum discussions (Bossler & Berenblum, 2019; Holt & Bossler, 2016). In an attempt to bridge the gap in the literature, this study explored the Chinese online community to understand online fraud victimization – in particular, to explore patterns in online fraud victimization cases.

The present study revealed several key research findings. First, while the relation between fraud types and victimization methods in the Baidu Tieba dataset is highly significant, types of social media shed light on different victimization methods. In addition, other mediums, except for phones, are known as new media/social media. Interesting differences exist between old and new media that are used for targeting victims in China. Specifically, refund frauds were primarily perpetrated through Alipay, which is a very popular system of e-payment. Online and mobile messengers that have e-payment functions, including WeChat and QQ, and the online shopping website Taobao are associated with two types of fraud techniques: return fraud and refund fraud. While return fraud is the predominant type for these three online venues, these mediums were also apparently associated with refund frauds. Exchanging goods and services online is done on the basis of trust; however, fraudsters exploit this basic tenet of online services to victimize targets. The fraudsters either do not return goods or services or do not pay the amount due; therefore, both return and refund frauds can be achieved rather easily. Another key research finding is that phones are still used either alone or in combination with other social media to defraud, particularly through phone bill fraud, card fraud, and fake contacts.

Second, victimization patterns correspond with the rapid pace of China's technological development, while a combination of online and traditional methods of perpetrating fraud still exist. This clearly indicates that not only does technology provide spaces for Chinese



criminals to develop their skills in victimizing innocent people, but also the Internet in particular can be used as a tool by victims who wish to share information with the public about criminals they have encountered. Both parties – those committing crimes and those reporting victimization – take advantage of anonymity online (Bouchard, 2016; Grant & Lavery, 2017). While fraud is certainly not a new phenomenon (Grabosky & Smith, 1998), the extent to which fraud has evolved and changed in recent years is significant. In particular, the evolution of the Internet and other digital technologies has drastically changed the ways in which fraud is perpetrated (Yar, 2013). Fraud is still committed in traditional, offline contexts, yet the Internet now facilitates a globally connected network of both victims and offenders who can potentially interact with each other (Button & Cross, 2017).

Third, a combination of mosaic plot, chi-square test, and MCA results indicate that Baidu Tieba functions as a common space for victims to report victimization and interact with other victims. The results show that the use of a particular type of social media, such as QQ or WeChat, significantly predicts the occurrence of specific types of online fraud. Exploring victims' behavioral traits for victimization, those who are more exposed online and in social media are also more suitable targets of online fraud. Expanding the risk of users being targeted, QQ – traditionally a PC-based messenger – now also has a mobile app. Together with QQ, Taobao – arguably the most famous and popular online shopping website in China – is used primarily for return and refund fraud owing to its predominant function being the exchange of messages and payments. Compared with these sites, the smartphone-based messenger and payment apps WeChat and Alipay are typically used for refund frauds.

This research contributes to the field by examining an understudied topic within existing literature on cybercrime, drawing from an underutilized data source. The current literature on cybercrime, especially regarding online fraud, tends to concentrate on specific countries and/or regions. The present study adds a different perspective to our understanding of online fraud by examining the relationships between various online platforms in China and online fraud methods.

This research is not without limitations, but the limitations could also be potential avenues for future research. This research is an important step forward in examining China's largest cybercrime-reporting markets. However, the sample size was rather small due to the availability of analyzable information in the data. Although the forum that was chosen was the largest possible arena to study, future research should consider combining different forums into a single dataset to be explored and analyzed. In future research, detailed qualitative content analysis of Baidu Tieba forums can also be studied to understand nuanced meanings and procedures of victimization online. With more longitudinal data and the reduction of missing information, other rigorous statistical methods – such as event history analysis – can be used to create extended datasets that cover longer periods of time.

This study presents the following implications for the future. First, users' characteristics are related their likelihood of being victims. From the demographic features of social media users, victims are usually young, and young users typically use social media such as QQ and WeChat. This has further implications for social media-related victimization and social media policing. Second, the current law regarding online frauds in China is often applicable only to cases where a victim has lost more than 2,000 RMB, or about 296 USD (Standing Committee of the National People's Congress, 2016). There is no systematic legal recourse for victims who have been scammed out of a smaller amount of money. Thus, it is especially important for people to be vigilant and careful when making any contracts or transactions

for goods and services online. Third, this research opens a research avenue and shows that innovative data collection methods can be used to examine cybercrime even in an understudied country, such as China. In conclusion, these findings provide not only theoretical and methodological implications, but also practical implications for online fraud in China and elsewhere.

This study identifies implications and policy measures, along with the significance of cybercrime, for authorities and citizens to address issues of digital media environments and cyberspace. Finally, authorities and citizens should understand the significance of cybercrime to address issues related to the environments of virtual communities and digital media and should take this data into account in forming future policy.

## Disclosure statement

No potential conflict of interest was reported by the author(s).

## ORCID

Claire Seungeun Lee  <http://orcid.org/0000-0002-0355-8793>

## References

- Abdi, H., & Valentin, D. (2007). Multiple correspondence analysis. In N. J. Salkind (Ed.), *Encyclopedia of measurement and statistics* (pp. 650–657). Sage.
- Baidu Tieba. (2018). Retrieved March 10, 2020, from <https://tieba.baidu.com/index.html>
- Blasius, J., & Thiessen, V. (2001). Methodological artifacts in measures of political efficacy and trust: A multiple correspondence analysis. *Political Analysis*, 9(1), 1–20. <https://doi.org/10.1093/oxfordjournals.pan.a004862>
- Bossler, A. M., & Berenblum, T. (2019). Introduction: New directions in cybercrime research. *Journal of Crime and Justice*, 42(5), 1–5. <https://doi.org/10.1080/0735648X.2019.1692426>
- Bouchard, K. L. (2016). Anonymity as a double-edge sword: Reflecting on the implications of online qualitative research in studying sensitive topics. *The Qualitative Report*, 21(1), 59–67. <https://nsuworks.nova.edu/tqr/vol21/iss1/5/>
- Buchanan, T., & Whitty, M. T. (2014). The online dating romance scam: Causes and consequences of victimhood. *Psychology, Crime & Law*, 20(3), 261–283. <https://doi.org/10.1080/1068316X.2013.772180>
- Button, M. & Cross, C. (2017). Technology and fraud: The ‘fraudogenic’ consequences of the Internet revolution. In T. J. Holt & M. R. McGuire (Eds.), *The Routledge handbook of technology crime and justice (Routledge International Handbooks)* (pp. 78–95). Routledge.
- Calderoni, F., Berlusconi, G., Garofalo, L., Giommoni, L., & Sarno, F. (2016). The Italian mafias in the world: A systematic assessment of the mobility of criminal groups. *European Journal of Criminology*, 13(4), 413–433. <https://doi.org/10.1177/1477370815623570>
- Chang, L. Y.-C. (2012). *Cybercrime in the greater China region: Regulatory response and crime prevention across the Taiwan strait*. Edward Elgar.
- Chen, J., Cumming, D., Hou, W., & Lee, E. (2016). Does the external monitoring effect of financial analysts deter corporate fraud in China? *Journal of Business Ethics*, 134(4), 727–742. <https://doi.org/10.1007/s10551-014-2393-3>
- Chen, J., Tao, Y., Wang, H., & Chen, T. (2015). Big data based fraud risk management at Alibaba. *Journal of Finance and Data Science*, 1(1), 1–10. <https://doi.org/10.1016/j.jfds.2015.03.001>
- China Internet Network Information Center. (2018). *Statistical Report on Internet Development in China (January 2018)*. CNNIC.

- China Internet Network Information Center. (2020). *Statistical Report on Internet Development in China (March 2020)*. CNNIC.
- Choi, K.-S., Lee, C. S., & Cadigan, R. (2018). Spreading propaganda in cyberspace: Comparing cyber-resource usage of al Qaeda and ISIS. *International Journal of Cybersecurity Intelligence & Cybercrime*, 1(1), 21–39. <https://vc.bridgew.edu/ijcic/vol1/iss1/4/>
- Clarke, R. V., & Felson, M. (1993). Introduction: Criminology, routine activity and rational choice. In R. V. Clarke & M. Felson (Eds.), *Routine activity and rational choice: Advances in criminological theory* (Vol. 5). Transaction Publishers, 1–14.
- Cohen, L., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588–608. <https://doi.org/10.2307/2094589>
- Conradt, C. (2012). Online auction fraud and criminological theories: The Adrian Ghighina case. *International Journal of Cyber Criminology*, 6(1), 912–923.
- Canyon, M. J., & He, L. (2016). Executive compensation and corporate fraud in China. *Journal of Business Ethics*, 134(4), 669–691. <https://doi.org/10.1007/s10551-014-2390-6>
- Costa, P. S., Santos, N. C., Cunha, P., Cotter, J., & Sousa, N. (2013). The use of multiple correspondence analysis to explore associations between categories of qualitative variables in healthy ageing. *Journal of Aging Research*, 2013, 1–12. <https://doi.org/10.1155/2013/302163>
- Cross, C. (2016). Using financial intelligence to target online fraud victimisation: Applying a tertiary prevention perspective. *Criminal Justice Studies*, 29(2), 125–142. <https://doi.org/10.1080/1478601X.2016.1170278>
- Cross, C. (2017). I've lost some sleep over it: Secondary trauma in the provision of support to older fraud victims. *Canadian Journal of Criminology and Criminal Justice*, 59(2), 168–197. <https://doi.org/10.3138/cjccj.2016.E11>
- Cross, C. (2018). (Mis)Understanding the impact of online fraud: Implications for victim assistance schemes. *Victims & Offenders*, 13(6), 757–776. <https://doi.org/10.1080/15564886.2018.1474154>
- Cross, C., & Kelly, M. (2016). The problem of 'white noise': Examining current prevention approaches to online fraud. *Journal of Financial Crime*, 23(4), 806–818. <https://doi.org/10.1108/JFC-12-2015-0069>
- Cross, C., Smith, R. G., & Richards, K. (2014). Challenges of responding to online fraud victimisation in Australia. *Trends and Issues in Crime and Justice*, (474), 1–6.
- Dolan, K. M. (2004). Internet auction fraud: The silent victims. *Journal of Economic Crime Management*, 2(1), 1–22.
- Fang, Z., Zhao, X., Wei, Q., Chen, G., Zhang, Y., Xing, C., Li, W., & Chen, H. (2016, September 28–30). *Exploring key hackers and cybersecurity threats in Chinese hacker communities*. 2016 IEEE Conference on Intelligence and Security Informatics (ISI), Tucson, Arizona, USA. <https://ieeexplore.ieee.org/abstract/document/7745436/authors#authors>
- Forum on Fraudsters (*Dapianzi ba*). (2018). *Baidu Tieba*. Retrieved November 21, 2018, from <http://tieba.baidu.com/f/good?kw=%B4%F3%C6%AD%D7%D3&fr=ala0&tpl=5>
- Franklin, J., Perrig, A., Paxson, V., & Savage, S. (2007). An inquiry into the nature and causes of the wealth of internet miscreants. In *ACM Conference on Computer and Communications Security* (pp. 375–388). Association for Computer Machinery.
- Frederick, B. J., & Perrone, D. (2014). "Party N play" on the internet: Subcultural formation, craigslist, and escaping from stigma. *Deviant Behavior*, 35(11), 859–884. <https://doi.org/10.1080/01639625.2014.897116>
- Gao, S., & Zhang, X. (2015). Understanding the use of location sharing services on social networking platforms in China. International conference on E-business and telecommunications (ICETE 2015). *E-Business and Telecommunications*, 124–136.
- Garg, V., & Nilizadeh, S. (2013). *Craigslist scams and community composition: Investigating online fraud victimization*. 2013 IEEE Security and Privacy Workshops, San Francisco, California, USA.
- Godes, D., & Mayzlin, D. (2004). Using online conversations to study word-of-mouth communication. *Marketing Science*, 23(4), 545–560. <https://doi.org/10.1287/mksc.1040.0071>
- Grabosky, P. N., & Smith, R. (1998). *Crime in the digital age: Controlling telecommunications and cyberspace illegalities*. Transaction Publishers.

- Grant, H., & Lavery, C. (2017). Masquerading sanity: Crimes, violence and victimization on the internet. *Acta Psychopathologica*, 3(3), 1–4. <https://doi.org/10.4172/2469-6676.100098>
- Grov, C. (2012). HIV risk and substance use in men who have sex with men surveyed in bathhouses, bars/ clubs, and on Craigslist.org: Venue of recruitment matters. *AIDS and Behavior*, 16(4), 807–817. <https://doi.org/10.1007/s10461-011-9999-6>
- Guo, Y., Bao, Y., Stuart, B. J., & Le-Nguyen, K. (2018). To sell or not to sell: Exploring sellers' trust and risk of chargeback fraud in cross-border electronic commerce. *Information Systems Journal*, 28(2), 359–383. <https://doi.org/10.1111/isj.12144>
- Hanson, A., & Hawley, Z. (2011). Do landlords discriminate in the rental housing market? Evidence from an internet field experiment in US cities. *Journal of Urban Economics*, 70(2–3), 99–114. <https://doi.org/10.1016/j.jue.2011.02.003>
- Hartigan, J. A., & Kleiner, B. (1981). *Mosaics for contingency tables*. Computer Science and Statistics: Proceedings of the 13th Symposium on the Interface (pp. 268–273), Pittsburgh, Pennsylvania, USA.
- Herold, D. K., & Marolt, P. (Eds.). (2011). *Online society in China: Creating, celebrating, and instrumentalising the online carnival*. Routledge.
- Hofmann, H. (2000). Exploring categorical data: Interactive mosaic plots. *Metrika*, 51(1), 11–26. <https://doi.org/10.1007/s001840000041>
- Hofmann, H. (2008). Mosaic plots and their variants. In C.-H. Chen, W. K. Haerdle, & A. Unwin (Eds.), *Handbook of data visualization* (pp. 617–642). Springer.
- Holt, T. J. (2012). Examining the forces shaping cybercrime markets online. *Social Science Computer Review*, 31(2), 165–177. <https://doi.org/10.1177/0894439312452998>
- Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge.
- Holt, T. J., Smirnova, O., & Chua, Y. T. (2016). Exploring and estimating the revenues and profits of participants in stolen data markets. *Deviant Behavior*, 37(4), 353–367. <https://doi.org/10.1080/01639625.2015.1026766>
- Hu, M. Y. (2004). Line mosaic plot: Algorithm and implementation. In J. Antoch (Ed.), *COMPSTAT 2004 — proceedings in computational statistics* (pp. 277–285). Physica. [https://doi.org/10.1007/978-3-7908-2656-2\\_22](https://doi.org/10.1007/978-3-7908-2656-2_22)
- Internet Crime Reporting Center (Wangluo weifa fanzui jubao wangzhan). (2015). Retrieved June 5, 2020, from <http://www.cyberpolice.cn/wfjb/html/index.shtml>
- Internet Crime Reporting Center (Wangluo weifa fanzui jubao wangzhan). (2016). Retrieved June 5, 2020, from <http://www.cyberpolice.cn/wfjb/html/index.shtml>
- Internet Crime Reporting Center (Wangluo weifa fanzui jubao wangzhan). (2017). Retrieved June 5, 2020, from <http://www.cyberpolice.cn/wfjb/html/index.shtml>
- Internet Crime Reporting Center (Wangluo weifa fanzui jubao wangzhan). (2018). Retrieved June 5, 2020, from <http://www.cyberpolice.cn/wfjb/html/index.shtml>
- Internet Crime Reporting Center (Wangluo weifa fanzui jubao wangzhan). (2019). Retrieved June 5, 2020, from <http://www.cyberpolice.cn/wfjb/html/index.shtml>
- Internet Crime Reporting Center (Wangluo weifa fanzui jubao wangzhan). (2020). Retrieved June 5, 2020, from <http://www.cyberpolice.cn/wfjb/html/index.shtml>
- Jiang, M. (2010). Authoritarian informationalism: China's approach to internet sovereignty. *SAIS Review of International Affairs*, 30(2), 71–89.
- King, G., Pan, J., & Roberts, M. E. (2013). How censorship in China allows government criticism but silences collective expression. *American Political Science Review*, 107(2), 1–18. <https://doi.org/10.1017/S0003055413000014>
- King, G., Pan, J., & Roberts, M. E. (2014). Reverse-engineering censorship in China: Randomized experimentation and participant observation. *Science*, 345(6199), 1–10. <https://doi.org/10.1126/science.1251722>
- Kroft, K., & Pope, D. G. (2014). Does online search crowd out traditional search and improve matching efficiency? Evidence from Craigslist. *Journal of Labor Economics*, 32(2), 259–303. <https://doi.org/10.1086/673374>

- Laforet, S., & Li, X. (2005). Consumers' attitudes towards online and mobile banking in China. *International Journal of Bank Marketing*, 23(5), 362–380. <https://doi.org/10.1108/02652320510629250>
- Lair, C. D., & Andrews, C. K. (2018). Advertising a particularly precarious occupation: Nanny ads on Craigslist. *Sociological Spectrum*, 38(2), 69–85. <https://doi.org/10.1080/02732173.2018.1430636>
- Lair, C. D., MacLeod, C., & Budger, E. (2016). Advertising unreasonable expectations: Nanny ads on Craigslist. *Sociological Spectrum*, 36(5), 286–302. <https://doi.org/10.1080/02732173.2016.1169236>
- Landis, J. R., & Koch, G. G. (1977). The measurement of observer agreement for categorical data. *Biometrics*, 33(1), 159–174. <https://doi.org/10.2307/2529310>
- Lee, C. S. (2020). A crime script analysis of transnational identity fraud: Migrant offenders' use of technology in South Korea. *Crime, Law, and Social Change*, 74(2), 201–218. <https://doi.org/10.1007/s10611-020-09885-3>
- Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior and Social Networking*, 17(8), 551–555. <https://doi.org/10.1089/cyber.2014.0008>
- Li, D., Li, J., & Lin, Z. (2008). Online consumer-to-consumer market in China – A comparative study of Taobao and eBay. *Electronic Commerce Research and Applications*, 7(1), 55–67. <https://doi.org/10.1016/j.elerap.2007.02.010>
- Li, L., Chen, Y.-W., & Nakazawa, M. (2013). Voices of Chinese web-TV audiences: A case of applying uses and gratifications theory to examine popularity of prison break in China. *China Media Research*, 9(1), 63–74.
- Liang, B., & Lu, H. (2010). Internet development, censorship, and cyber crimes in China. *Journal of Contemporary Criminal Justice*, 26(1), 103–120. <https://doi.org/10.1177/1043986209350437>
- Lin, Z., & Li, J. (2005, August 15–17). *The online auction market in China: A comparative study between Taobao and eBay*. Proceeding ICEC '05 Proceedings of the 7th International conference on Electronic commerce (pp. 123–129), Xi'an.
- Liu, C., & Lu, X. (2018). Analyzing hidden populations online: Topic, emotion, and social network of HIV-related users in the largest Chinese online community. *BMC Medical Informatics and Decision Making*, 18(2). <https://doi.org/10.1186/s12911-017-0579-1>
- Liu, Y. (2006). Word of mouth for movies: Its dynamics and impact on box office revenue. *Journal of Marketing*, 70(July), 74–89. <https://doi.org/10.1509/jmkg.70.3.074>
- Lu, H., Liang, B., & Taylor, M. (2010). A comparative analysis of cybercrimes and governmental law enforcement in China and the United States. *Asian Journal of Criminology*, 5(2), 123–135. <https://doi.org/10.1007/s11417-010-9092-5>
- Maimon, D., Santos, M., & Park, Y. (2019). Online deception and situations conducive to the progression of non-payment fraud. *Journal of Crime and Justice*, 42(5), 516–535. <https://doi.org/10.1080/0735648X.2019.1691857>
- Marolt, P., & Herold, D. K. (2015). *China online: Locating society in online spaces*. Routledge.
- Mears, D. P., Reisig, M. D., Scaggs, S., & Holtfreter, K. (2016). Efforts to reduce consumer fraud victimization among the elderly: The effect of information access on program awareness and contact. *Crime and Delinquency*, 62(9), 1235–1259. <https://doi.org/10.1177/0011128714555759>
- Meng, B. (2011). From steamed bun to grass mud horse: E Gao as alternative political discourse on the Chinese internet. *Global Media and Communication*, 7(1), 33–51. <https://doi.org/10.1177/1742766510397938>
- Moskowitz, D. A., & Seal, D. W. (2010). “GWM looking for sex—serious only”: The interplay of sexual ad placement frequency and success on the sexual health of “men seeking men” on Craigslist. *Journal of Gay & Lesbian Social Services*, 22(4), 399–412. <https://doi.org/10.1080/10538720.2010.491744>
- Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011, November 2–4). *An analysis of underground forums*. IMC'11, Berlin, Germany.
- Oliveri, R. C. (2010). Discriminatory housing advertisements on-line: Lessons from craigslist. *Indiana Law Review*, 43, 1125–1183.



- Park, Y., Jones, J., McCoy, D., Shi, E., & Jakobsson, M. (2014). *Scambaiter: Understanding targeted Nigerian scams on craigslist*. NDSS Symposium 2014, San Diego, California, USA.
- 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. <https://doi.org/10.1177/0022427810365903>
- Radbod, S. T. (2010). Craigslist - A case for criminal liability for online service providers? *Berkeley Technology Law Journal*, 25, 597–615.
- Rege, A. (2009). What's love got to do with it? Exploring online dating scams and identity. *International Journal of Cyber Criminology*, 3(2), 494–512.
- Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency*, 50(2), 216–238. <https://doi.org/10.1177/0022427811425539>
- Robinson, B. A., & Vidal-Ortiz, S. (2013). Displacing the dominant “down low” discourse: Deviance, same-sex desire, and Craigslist.Org. *Deviant Behavior*, 34(3), 224–241. <https://doi.org/10.1080/01639625.2012.726174>
- Rosenbaum, M. S., Daunt, K. L., & Jiang, A. (2013). Craigslist exposed: The internet-mediated hookup. *Journal of Homosexuality*, 60(4), 505–531. <https://doi.org/10.1080/00918369.2013.760305>
- Schackman, D. (2010). Commons or gated community? A theoretical explication of virtual community and the example of Craigslist. *Journal of Community Informatics*, 6(2).
- Song, X.-P., Hu, Z.-H., Du, J.-G., & Sheng, Z.-H. (2014). Application of machine learning methods to risk assessment of financial statement fraud: Evidence from China. *Journal of Forecasting*, 33(8), 611–626. <https://doi.org/10.1002/for.2294>
- Standing Committee of the National People's Congress. (2016). *Cybersecurity law of the People's Republic of China*. Effective date: June 1, 2017.
- Stockmann, D., & Luo, T. (2017). Which social media facilitate online public opinion in China? *Problems of Post-Communism*, 64(3–4), 189–202. <https://doi.org/10.1080/10758216.2017.1289818>
- Sullivan, J., & Xie, L. (2009). Environmental activism, social networks, and the internet. *The China Quarterly*, 198, 422–432. <https://doi.org/10.1017/S0305741009000381>
- Tofighi, B., Perna, M., Desai, A., Gorv, C., & Lee, J. D. (2016). Craigslist as a source for heroin: A report of two cases. *Journal of Substance Use*, 21(5), 543–546. <https://doi.org/10.3109/14659891.2015.1090495>
- 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. <https://doi.org/10.1093/esr/jcr053>
- Wehinger, F. (2011). The dark net: Self-regulation dynamics of illegal online markets for identities and related services. *Intelligence and Security Informatics Conference*, 209–213.
- Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. *Cyberpsychology, Behavior and Social Networking*, 15(3), 181–183. <https://doi.org/10.1089/cyber.2011.0352>
- Wu, L., Zhang, J., & Zhao, M. (2014). The metabolism and growth of web forums. *PLoS One*, 9(8). <https://doi.org/10.1371/journal.pone.0102646>
- Xu, Y. (2016). Research on the application of informational investigation to WeChat fraud case (*Xinxihua zhencha zai weixin zhaphian anjian zhong de yingyong tanxi*). *Journal of Hunan Police Academy*, 28(3), 35–40.
- Yang, G. (2011). *The power of the internet in China: Citizen activism online*. Columbia University Press.
- Yang, J., Cheng, L., & Luo, X. (2009). A comparative study on e-banking services between China and USA. *International Journal of Electronic Finance*, 3(3), 235–252. <https://doi.org/10.1504/IJEF.2009.027848>
- Yar, M. (2013). *Cybercrime and society*. Sage.
- Ye, N. (2004). Dimensions of consumer's perceived risk in online shopping. *Journal of Electronic Science and Technology of China*, 2(3), 177–182.
- Yip, M. (2011, June 14–17). *An investigation into Chinese cybercrime and the applicability of social network analysis*. ACM WebSci '11, Koblenz, Germany. [https://eprints.soton.ac.uk/272351/2/yip\\_poster\\_2011.pdf](https://eprints.soton.ac.uk/272351/2/yip_poster_2011.pdf)



- Yoon, C. (2010). Antecedents of customer satisfaction with online banking in China: The effects of experience. *Computers in Human Behavior*, 26(6), 1296–1304. <https://doi.org/10.1016/j.chb.2010.04.001>
- Yuan, J., & Ye, Z. (2016). Causes of WeChat fraud crime and countermeasures (Weixinzhapianfanzui de zhenchakunjing he pojieduicefenxi: Jiyu weixinzhapianfanzuianjiande xianshikaocha). *Journal of Hebei Vocational College of Public Security Police*, 16(2), 21–26.
- Zahedi, M. Z., Abbasi, A., & Yan, C. (2015). Fake-website detection tools: Identifying elements that promote individuals' use and enhance their performance. *Journal of the Association for Information Systems*, 16(6). <https://aisel.aisnet.org/jais/vol16/iss6/2>
- Zhang, Y., Bian, J., & Zhu, W. (2013). Trust fraud: A crucial challenge for China's e-commerce market. *Electronic Commerce Research and Applications*, 12(5), 299–308. <https://doi.org/10.1016/j.elerap.2012.11.005>