World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:15, No:4, 2021

Journey to Cybercrime and Crime Opportunity: Quantitative Analysis of Cyber Offender Spatial Decision Making

Sinchul Back, Sun Ho Kim, Jennifer LaPrade, Ilju Seong

***Abstract*—**Due to the advantage of using the Internet, cybercriminals can reach target(s) without border controls. Prior research on criminology and crime science has largely been void of empirical studies on journey-to-cybercrime and crime opportunity. Thus, the purpose of this study is to understand more about cyber offender spatial decision making associated with crime opportunity factors (i.e., co-offending, offender-stranger). Data utilized in this study were derived from 306 U.S. Federal court cases of cybercrime. The findings of this study indicated that there was a positive relationship between co-offending and journey-to-cybercrime, whereas there was no link between offender-stranger and journey-to-cybercrime. Also, the results showed that there was no relationship between cybercriminal sex, age, and journey-to-cybercrime. The policy implications and limitations of this study are discussed.

***Keywords*—**Co-offending, crime opportunity, journey-to-cybercrime, offender-stranger

I. Introduction

SOME circumstances and situational factors of crime targets could serve to increase criminal opportunities by making offenders more capable to effectively commit crime and raise the suitability of the target. Previous studies [1]-[4] indicate that some situational/opportunity factors influenced the characteristics of cybercrime scenes. For example, there is a relationship between pre-crime situational factors (such as political objective presence) and characteristics of cybercrime scenes. Also, these studies found that certain cybercrime opportunity factors – (1) offender's distance from target, (2) type of target, and (3) intimate relationship with target – were significant predictors of cybercrime incidents. Remarkably, cyber offenders tended to select and attack targets in different jurisdictions (different countries or states) and targets' physical location are farther from where they live [5]. This pattern creates increased difficulties for cybercrime investigation and prosecution. Furthermore, these findings are contrary to studies examining other types of crime [6]-[10] where results show that offenders in the physical world tend to commit crimes close to where he or she lives.

Sinchul Back is with the University of Scranton (e-mail: sinchul.back@scranton.edu).
Sun Ho Kim is with Indiana University, United States (e-mail: kimsunh@iu.edu).
Jennifer LaPrade is with Missouri State University (e-mail: JLaPrade@missouristate.edu).
Ilju Seong is with Centennial College (e-mail: iseong@my.centennialcollege.ca).

Due to the borderless nature of cybercrime, cyber perpetrators can more easily victimize many people all over the globe including the United States. They can commit cybercrime more severely and anonymously without ever setting foot in the targeted victim's location. Grabosky [11] and Chang [12] asserted that cyber offenders attempt to conceal their physical location through a number of jurisdictions on the way to their target. Sophisticated cybercriminals have more opportunities to reach targets over the Internet from the nations called safe havens where cybercrime investigation treaties, extradition, law enforcement cooperation, and technical capacity are absent in order to hide in the shadows of the Internet.

In a related sense, cyber offenders' geospatial behaviors differ from offenders in the physical world due to the collapse of spatial and temporal orderings. However, offender- and victim- physical locations are still crucial factors to effectively prosecute cybercrime incidents and to reduce cybercriminal opportunities. Despite the importance of offenders' geospatial behaviors and crime opportunity, to date few studies have conducted research on crime opportunity and journey-to-cybercrime factors. Therefore, this study adds to the literature to help scholars and practitioners understand cyber offenders' spatial decision making and the factors that may increase the likelihood of crossing jurisdictional boundaries to commit cybercrime. This study seeks to empirically examine a relationship between crime opportunity and journey-to-cybercrime in order to help law enforcement predict future cybercriminal's geospatial behaviors and to create an effective cybercrime prevention strategy nationally and globally. With that in mind, this study will outline the literature review, methodology, as well as present the results of the analysis. Lastly, this study will discuss the findings, policy implications, and limitations of this research.

II. Literature Review

A. Crime Opportunity and Journey-to-Cybercrime

Crime opportunity theory asserts that criminals are motivated and the availability of opportunity – whether they actively seek it or they stumble upon it – determines the occurrence of a crime [13]. According to [13], opportunity factors play a significant role in the development of crime, crime method selection, and/or finding a suitable target. Another explanation of crime opportunity is provided by routine activities theory. Routine activities theory (RAT), first offered by Cohen and Felson [14], emphasizes three elements

that need to converge in time and space for crime to occur: motivated offender, suitable target, and lack of guardianship. As a rational decision process, potential offenders generally select attractive targets that are easily accessible and that can give them the satisfaction of rewards they seek. These crime opportunity factors were found to be important predictors of offender spatial decision making along with selecting victim/ target(s) and committing crime [4], [15]. Importantly, [4] and [16] suggest that (1) *co-offending* and (2) *offender knew victim* prior to committing crime (offender-stranger) factors may serve as opportunity factors in the commission of the crime process as well as selecting target(s) before the course of the attack [17], [18].

Many criminologists assert that most crimes occur near locations where the criminal is familiar or knowledgeable. For example, [19] explains that most criminal activities occur near where offenders live or work; however, with a buffer zone around the offender's residence where the offender is less likely to commit a crime due to fear of being easily recognized and apprehended [20], [21]. In the same sense, [22] argues that distance estimation is a significant factor when offenders in the physical world shape their crime location choices and spatial behaviors prior to committing the crime. Back et al. [23] found that due to the collapse of spatial distance there is no spatial border between the motivated offender and suitable target in line with an application of RAT in cyberspace. In other words, cyber offenders can commit crimes against targets in different real-world time zones without any border controls.

Morselli and Royer [24] and Clarke and Cornish [25] argue that criminal mobility should also be considered a goal-oriented action (e.g., offenders who travel farther to commit their crimes had good reasons to do so). For example, criminal mobility might serve the goal of successfully completing the crime and avoiding detection [26], [27]. In a study of cyberattacks, Holt and Kilger [28] conclude that cyber offenders prefer to commit cyberattacks against a foreign country's critical infrastructures and they tend to carefully prepare attacks against their targets. However, there may exist hurdles (e.g., languages barriers, different network systems, and various cybersecurity countermeasures) needed to overcome when cyber offenders attack target/victim(s) located in other cities, states, and/or countries. To overcome these barriers, increasing crime opportunity may be a good remedy to help complete their malicious goals. In this regard, [4] asserts that *co-offending* and *offender knew target* prior to committing crime (offender-stranger) may provide special opportunities because these factors can create more favorable conditions to commit crimes. Thus, it is clear that based on crime opportunity, cyber offenders may be prone to travel farther to commit crimes if they achieve their objectives such as more monetary gain and efficiently avoiding prosecution by law enforcement due to the jurisdiction issues. Taken together, these ideas seem to offer an explanation for why and how crime opportunity could affect offender spatial decision making prior to committing crime.

III. Present Study

The prior research suggests that crime opportunity factors can influence offender spatial decision making to commit cybercrime in virtual settings. Given this situation, cyber offenders may be prone to virtually travel farther to commit crime with more opportunities such as co-offending and offender-stranger. With this reasoning, the current study seeks to examine the relationship between cyber offender spatial decision making and crime opportunity before the cybercrime event.

- Research question: Is opportunity a predictor of offender spatial decision making in cyberspace?
- Hypothesis [H1]: Co-offending opportunities will be positively related to farther virtual distance traveled to commit cybercrimes.
- Hypothesis [H2]: Familiarity with the target will be positively related to farther virtual distance traveled to commit to cybercrimes.

IV. Methodology

A. Data

Data were extracted from the Florida International University Law library website concerning cybercrime offense convictions. One database used for the foundation of the search was the Bloomberg Law for Case Dockets Research which contains federal and state court dockets and access case filings. To collect criminal record reports (i.e., indictment, complaints), the following terms were utilized for the query: cyber-fraud, hacking, cyberattack, online sexual crime, online illicit trade, cyberstalking, and cyberbullying, returning 1,829 federal court cases. Each case was read, and this search revealed 306 U.S. Federal court cases of cybercrime occurring between 2001 and 2018 which were used to empirically investigate the cyber-criminal profiling framework.

To collect quantitative data, the Dyadic Cyber Incident and Dispute (DCID) Dataset, Version 1.5 Incident framework variables [29] was employed to provide coding and interpretation of available variables applied to the 306 court cases. In fact, the DCID was able to provide the operational ideas of the variables, including offenses and offenders' information (i.e., age, gender, nationality, geographic information of offender, type of cyber interaction for incidents, cyberattack methods utilized, type of target by cybercriminal, objective success, severity level of cybercrime, and damage type). The following sections explain the dependent and independent variables as well as the analytic plan.

B. Dependent Variable

The current study focuses on measuring a dependent variable, *offender distance from victim or target*. Based on the codebook derived from [30], scaling for jurisdictional distance between offender and target locations are as follows: intracity level (1 = intracity level), intercity level (2 = intercity level), interstate level (3 = interstate level), and international level (4 = international level).

C. Independent Variables

As stated in the literature review, [4] and [31] have postulated a direct relationship between the personal

characteristics of offender, the crime opportunity for offender, and the characteristics of crime scenes. Consistent with [4], the current study employed two items to measure individual characteristics of the cybercrime opportunity.

First, to measure *characteristics of cybercrime opportunities*, two variables were utilized: (1) presence of co-offenders; (2) offender-stranger. Scaling for presence of co-offender is as follows: 0 = no, 1 = yes. Scaling for offender-stranger is as follows: 0 = no, 1 = yes. Then, *sociodemographic background factors* were measured using four variables: sex and age. Sex was coded as 0 = female and 1 = male. Age is a continuous variable ranging from 18 to 68 years.

D. Analytic Method

All models were estimated using SPSS 27. First, a descriptive statistic of variables was shown. Second, a series of Ordinary Least Squares (OLS) regressions were employed in order to test the hypothesis concerning the association between crime opportunity and journey-to-cybercrime. The OLS regression models were suitable to analyze these data since the relationship between the independent variables and dependent variable was linear. The Shapiro-Wilk test and Kolmogorov-Smirnov Test (K-S Test) determined that the dependent variable was normally distributed (Shapiro-Wilk test: $p > 0.05$; 1-Sample Kolmogorov-Smirnov Test: $p > 0.05$) [32]. In addition, all the tolerance values are over 0.20 and all the variance inflation factor (VIF) statistics are less than 10; therefore, there is no problem for multicollinearity among variables. The analyses began with a bivariate regression where the co-offending variable is modeled as the sole predictor of journey-to-cybercrime in order to obtain a baseline association. Next, demographic variables (i.e., gender and age) were added to the OLS regression model. Finally, the offender-stranger variable was added to the model.

V. Results

A. Descriptive Statistical Analysis

Descriptive analyses were performed to demonstrate the sample characteristics and responses to the candidate variables. Table I provides the descriptive statistics (i.e., minimum and maximum counts, means, standard deviations, and a number of the sample) for each dependent and independent variable in the multivariate analyses in this study.

TABLE I
DESCRIPTIVE STATISTICS: SSBACO VARIABLES

Variables	Mean	SD	Min	Max
Sociodemographic Factors				
Offender sex (male = 1)	0.94	0.24	0	1
Offender age	34.24	9.95	18	68
Cybercrime Opportunity				
Presence of co-offenders	0.63	0.48	0	1
Offender knew victim/target	0.40	0.49	0	1
Dependent Variable				
Jurisdictional distance between offender and target	2.80	1.07	1	4

B. OLS Regression Results of Journey-to-Cybercrime

Table II presents the results of the series of OLS regression analyses conducted in order to investigate the hypotheses. Model 1 shows that there was a statistically significant, positive relationship between co-offending and journey-to-cybercrime ($b = 1.16$, SE = 0.11, $\beta = 0.51$, $p < 0.001$). This finding indicates that individuals with co-offender(s) were more likely to travel farther which is the predicted direction of hypothesis 1. Model 2 adds the demographic variables to account for differences in gender and age. As shown, both gender and age variables were not significant predictors of journey-to-cybercrime.

TABLE II
OLS REGRESSION RESULTS PREDICTING JOURNEY-TO-CYBERCRIME (N= 306)

	Model 1		Model 2		Model 3	
Variables	*b*	SE	*b*	SE	*b*	SE
Co-offending	1.16***	0.11	1.17***	0.11	1.13***	0.11
Offender-stranger					0.29	0.004
Gender			0.10	0.22	0.08	0.22
Age			0.01	0.005	0.01	0.005
R^2	0.27		0.27		0.28	

*** $p < .001$

As predicted, Model 3 shows that co-offending factor was positively associated with journey-to-cybercrime, while offender-stranger factor was not a significant predictor of journey-to-cybercrime. Specifically, individuals with co-offender(s) were 113% more likely to travel farther to commit cybercrime ($b = 1.13$., $SE = 0.11$, $\beta = 0.21$, $p < 0.001$), when compared to individuals without co-offender(s). In short, the results found support for hypothesis 1 but did not find support for hypothesis 2.

VI. Discussion and Conclusion

While the existing literature has empirically examined the link between crime opportunity and the journey-to-crime framework, few studies have conducted empirical research regarding its link in the virtual setting. Therefore, this study sought to investigate the link between crime opportunity factors – presence of co-offenders and offender-stranger – and journey-to-cybercrime factor.

First and foremost, findings support the presence of co-offenders in the cybercrime against target(s) farther from their location, which indicates that accomplices play a role in cybercrime across lengthy spatial distances. This may mean that while cyber criminals can reach victims of any distance, the opportunity to carry out the attacks against victims far away, in different regions and continents of the word, arises when there are more people involved in the attack. Second, findings also suggest that, for cybercrime, the commission of cybercrime may not require the pre-condition (offenders knew their specific targets) prior to victimization. While this finding contradicts the major tenet of RAT, it is in support of the cyber routine activity theory, that the convergence of the offender and the victim is not necessary for the crime to occur. In short, crime opportunity in the form of co-offending increases the likelihood of cyber offenders reaching across the globe in order

to achieve their malicious objectives.

VII. Policy Implications

The results of this study provide strong policy implications for authorities fighting against cybercrime in the United States and around the world. According to this study, cybercrime perpetrators will carry out an attack on any target across the world regardless of state borders, as long as there is an opportunity. And having an accomplice is a strong indicator of targeting systems far from their location. An accomplice is an element that can support and/or guide criminals to discover the opportunity and carry out the intended crime. For example, accomplices would be anyone who provides information about a suitable target that was previous unknown and those who provide tools and techniques to carry out the attack against the target.

Cyber criminals are often members of a secretive community that are connected through a tight network. They communicate through web forums, blogs, and other online communication venues, where they share information and sell-buy malicious programs and data [33]. Holt et al. [33] also found that some were members across different community sites, creating a network across different forums that allows the information and data to cross one another. And each of these small communities relies on few highly-skilled hackers who share their knowledge, techniques, and tools to their less-skilled counterparts. Through these communities the less-skilled hackers gain knowledge and experience of various tools, some of which they will acquire as their new skillset [34]. While the purpose of these online communities is mostly for sharing information and data, it is hard to overlook the possibility of the members to find co-offender(s) who have the specific skillsets that they themselves do not hold. Therefore, it is imperative to seek and identify these online communities to gather information on the individuals active in the community and on any critical information that may suggest a serious attack on any subject, including state government branches, public and private infrastructures, private industries, and the mass general population.

VIII. Limitations

Although this study provides insight into why and how crime opportunity could affect offender spatial decision making prior to committing crime, it is important to acknowledge a limitation of the study. The analysis relied on crime opportunity variables to measure journey-to-cybercrime pattern. Thus, it is possible that in some cases, cyber offenders might be prone to travel farther in order to disrupt law enforcement's investigation because they are likely to hide their physical location through a number of jurisdictions on the way to their target. As such, it might be limited to conceal a significant predictor of offender spatial decision-making process. Future research should address this issue by applying prolific sources in order to provide an in-depth understanding of the link between cybercrime opportunity and journey-to-crime.

References

[1] W. L. Marshall, and H. E. Barbaree, "An integrated theory of the etiology of sexual offending," in *Handbook of Sexual Assault* , W. L. Marshall, D. R. Laws, and H. E. Barbaree Eds. Boston, MA: Springer, 1990, pp. 257-275.

[2] C. M. Earls, and W. L. Marshall, "The current state of technology in the laboratory assessment of sexual arousal patterns," in I. R. Greer and J. G. Stuart Eds. *The Sexual Aggressor: Current Perspectives on Treatment*, New York : Van Nostrand Reinhold, 1983, pp. 336-362.

[3] C. G. Salfati, "The nature of expressiveness and instrumentality in homicide: Implications for offender profiling," *Homicide Studies*, vol. 4, no. 3, pp. 265-293, 2000.

[4] E. Beauregard, P. Lussier, and J. Proulx, "Criminal propensity and criminal opportunity," in *Criminal Profiling*, R. N. Kocsis, Ed. New Jersey: Humana Press, 2008, pp. 89-113.

[5] L. I. Hadzhidimova, and B. K. Payne, "The profile of the international cyber offender in the US," *International Journal of Cybersecurity Intelligence & Cybercrime*, vol. 2, no. 1, pp. 40-55, 2019.

[6] R. L. Block, and C. R. Block, "Space, place and crime: Hot spot areas and hot places of liquor-related crime,". *Crime and place*, vol. 4, no. 2, pp. 145-184, 1995.

[7] D. V. Canter, and A. Gregory, "Identifying the residential location of rapists," *Journal of the Forensic Science Society*, vol. 34, no. 3, 169-175, 1994.

[8] H. Jahankhani, and A. Al-Nemrat, "Examination of cyber-criminal behaviour," *International Journal of Information Science and Management (IJISM)*, pp. 41-48, 2012.

[9] S. Sarangi, and D. Youngs, "Spatial patterns of Indian serial burglars with relevance to geographical profiling," *Journal of Investigative Psychology and Offender Profiling*, vol. 3, no. 2, pp. 105-115, 2006.

[10] R. Jansen, and P. Van Koppen, "The road to robbery," *British Journal of Criminology*, vol. 38, no. 2, pp. 230-246, 1998.

[11] P. Grabosky, *Keynotes in criminology and criminal justice series: Cybercrime*. New York: Oxford University Press, 2015.

[12] L. Y. Chang, "Formal and informal modalities for policing cybercrime across the Taiwan Strait," *Policing and Society*, vol. 23, no. 4, pp. 540-555, 2013.

[13] M. Felson, and R. V. Clarke, "Opportunity makes the thief: Practical theory for crime prevention," *Police research series, paper 98*, pp. 1-36, 1998.

[14] L. E. Cohen and M. Felson, "Social change and crime rate trends: A routine activity approach," *American Sociological Review*, vol. 44, pp. 588-608, 1979.

[15] A. N. Hewitt, J. Chopin, and E. Beauregard, "Offender and victim 'journey-to-crime': Motivational differences among stranger rapists," *Journal of Criminal Justice*, vol. 69, article 101707, pp. 1-10, 2020.

[16] R. T. Guerette, S. A. Santana, "Explaining victim self-protective behavior effects on crime incident outcomes: A test of opportunity theory," *Crime & Delinquency*, vol. 56, no. 2, pp. 198-226, 2010.

[17] D. W. Osgood, J. K. Wilson, P. M. O'malley, J. G. Bachman, and L. D. Johnston, "Routine activities and individual deviant behavior," *American Sociological Review*, vol. 61, no. 4, pp. 635-655, 1996.

[18] M. Warr, "Crime and opportunity: A theoretical essay," in *The Process and Structure of Crime: Criminal Events and Crime Analysis*, *Advances in Criminological Theory series* vol. 9, R. F. Meier, L. W. Kennedy, and V. F. Sacco, Eds. New York: Routeledge, 2001, pp. 65-94.

[19] P. L. Brantingham, and P. J. Brantingham, "Situational crime prevention in practice," *Canadian Journal of Criminology*, vol. 32, pp. 17-40, 1990.

[20] D. K. Rossmo, L. Velarde, "Geographic profiling analysis: principles, methods and applications" in *Crime Mapping Case Studies: Practice and Research*, S. Chainey and L. Thompson Eds. West Sussex: John Wiley & Sons Ltd., 2008, pp. 35-43.

[21] R. Block, A. Galary, and D. Brice, "The journey to crime: Victims and offenders converge in violent index offences in Chicago," *Security Journal*, vol. 20, no. 2, 123-137, 2007.

[22] D. Canter, and L. Hammond, "A comparison of the efficacy of different decay functions in geographical profiling for a sample of US serial killers," *Journal of Investigative Psychology and Offender Profiling*, vol. 3, no. 2, pp. 91-103, 2006.

[23] S. Back, J. LaPrade, and S. Soor, "Spatial and Temporal Patterns of Cyberattacks: Effective CYBERCRIME Prevention Strategies around the Globe," *International Journal of Protection, Security & Investigation*, vol. 3, pp. 7-13, 2018.

[24] C. Morselli, and M. N. Royer, "Criminal mobility and criminal

achievement," *Journal of Research in Crime and Delinquency*, vol. 45, no. 1, pp. 4-21, 2008.
[25] R. V. Clarke, and D. B. Cornish, "Rational choice," in *Explaining Criminals and Crime: Essays in Contemporary Criminological Theory*, in R. Paternoster and R. Bachman Eds. New York: Oxford University Press, 2001, pp. 23-42.
[26] E. Beauregard, I. Busina, I. "Journey "during" crime: Predicting criminal mobility patterns in sexual assaults," *Journal of Interpersonal Violence*, vol. 28, no. 10, pp. 2052-2067, 2013.
[27] R. R. Hazelwood, and J. I. Warren, "Linkage analysis: Modus operandi, ritual, and signature in serial sexual crime," *Aggression and Violent Behavior*, vol. 9, pp. 307–318, 2004.
[28] T. J. Holt, M. Kilger, "Examining willingness to attack critical infrastructure online and offline," *Crime & Delinquency*, vol. 58, no. 5, pp. 798-822, 2012.
[29] R. Maness, B. Valeriano, and B. Jensen, "The dyadic cyber incident and campaign (DCID) dataset, version 1.5," 2019. Retrieved from http://www.brandonvaleriano.com/uploads/8/1/7/3/81735138/dcid_1.5_codebook.pdf
[30] S. Back, "The cybercrime triangle: An empirical assessment of offender, victim, and place", (Unpublished doctoral dissertation).
[31] R. M. Holmes, and S. T. Holmes, *Profiling violent crimes: An investigative tool*, 4th ed. Thousand Oaks, CA: Sage, 2008.
[32] C. Flatt, and R. L. Jacobs, "Principle Assumptions of Regression Analysis: Testing, Techniques, and Statistical Reporting of Imperfect Data Sets. *Advances in Developing Human Resources*, vol. 21, no. 4, pp. 484-502, 2019.
[33] T. J. Holt, D. Strumsky, O. Smirnova, and M. Kilger, "Examining the social networks of malware writers and hackers," *International Journal of Cyber Criminology*, vol. 6, no. 1, pp. 891-903, 2012.
[34] A. E. Voiskounsky, and O. V. Smyslova, "Flow-based model of computer hackers' motivation," *CyberPsychology & Behavior*, vol. 6, no. 2, pp. 171-180, 2003.