



Analyzing Cyber Violence in China from the Perspective of Routine Activity Theory

Ran Xu*

Criminology, Department of Sociology, The University of Hong Kong, Hong Kong, China

*1348713498@qq.com

Abstract. This article aims to analyze the phenomenon of cyber violence in China using Routine Activity Theory (RAT). The article first introduces the connotation of RAT and its strengths and weaknesses. RAT posits that three elements are necessary for a crime to occur: a motivated offender, a suitable target, and a lack of guardianship. This theory highlights the role of victims in crime and provides a new perspective for crime prevention, but it falls short in explaining the motives of crime. Regarding the motivations for cyber violence, some netizens, due to lower levels of education and income, poor self-control, and the weakening of moral constraints due to online anonymity, are prone to become bullies. In terms of suitable targets, frequent internet use, excessive exposure of personal information, high social engagement, and the concept of "tolerance" in traditional culture all increase the risk of victimization. Regarding guardianship, lapses in network platform management, inadequate operability of laws and regulations, and difficulties in law enforcement and rights protection lead to a lack of effective supervision in cyberspace.

Keywords: Routine Activity Theory, Cyber Violence, Motivated Offender, Suitable Targets, Absence of Regulation

1 Introduction

Routine Activity Theory (RAT) is an important theory in criminology proposed by Cohen and Felson in 1979. They attempted to understand the post-World War II rise in crime rates in the U.S., by examining patterns in people's routine activities. They assumed that changes in routine activities since World War II have resulted in more people appearing at specific times and places, increasing the possibility of their victimization. This hypothesis is confirmed in the study of crime hotspots by Sherman and others¹ (1989). Cohen and Felson² (1979) assumed three primary variables for criminal victimization: motivated offenders, suitable targets, and the lack of capable guardians. However, they did not explicitly define what constitutes a capable guardian. Sun and his colleagues³ (2022) suggest that capable guardianship can be measured by whether neighbors watch over the property and the intensity of street lighting etc. Cohen and Felson² (1979) propose that direct-contact predatory offenses are more likely to occur

when these three essential elements come together in both time and space. These elements are present to varying degrees in different environments, thus leading to variations in the risk of criminal victimization. In China, early one-third of people claim to have been victims of cyber violence, while nearly one-fifth admit to committing cyber violence⁴ (Jing & Hu, 2021). This essay aims to analyze the advantages and disadvantages of RAT, and apply it to explain the phenomenon of cyber violence in China.

2 Advantages

Firstly, one of the advantages of RAT is its simplicity and ease of understanding. The theory constructs a basic framework for explaining crime using just three core elements, and it integrates experiences and common sense from people's daily lives, making it widely accepted and applicable.

Secondly, RAT emphasizes the role of the victim in crime. Many traditional criminology theories prefer to analyze from the perspective of the offenders, such as their biological, psychological, and social factors, while relatively neglecting the victim. In contrast, RAT takes into account how the lifestyle of victims increases their vulnerability to victimization. For example, frequently walking alone at night can increase a person's risk of being robbed^{5,6} (Kennedy & Forde, 1990; AlKheder et al., 2022).

Thirdly, RAT provides useful perspectives for government policy-making. For example, in urban planning and architectural design, it is important to consider adding street lights, installing cameras, and creating defensible spaces in public buildings to enhance formal social control⁷ (Newman, 1973). Meanwhile, strengthening community building and encouraging residents to participate in community affairs can help increase the level of informal surveillance⁸ (Perkins et al., 1990). Unemployment and poverty can increase some people's motivation to commit crimes, so improving the social security system can reduce the number of potential offenders^{9,10} (Griffiths et al., 2004; Webster, 2023). These encourage more focus on crime prevention to reduce the occurrence of crime, rather than solely relying on the criminal justice system's punishment and deterrence.

Fourthly, RAT effectively explains how changes in social structure can affect direct-contact predatory crimes. For instance, economic development and urbanization lead to more people working outside the home, increasing the amount of time rural houses are left unoccupied and unguarded during the day, which raises the risk of burglaries¹¹ (Moriarty & Williams, 1996).

Finally, as research continues to deepen, RAT can be widely applied and fully developed in the study of various crimes, such as drug crime, teenage crime, white-collar crime, and even cybercrime^{12,13,14,15} (Marcum, 2011; Gottschalk, 2019; Akdemir & Lawless, 2020; de Jong et al., 2020).

3 Limitation

Firstly, although RAT is widely applied, it cannot explain negligence crime. For example, cases of death due to negligence, such as traffic accidents and medical mishaps.

Their occurrence is often due to negligence rather than an offender's premeditated choice of target and assessment of risks, and there is no offender motive involved.

Secondly, the variable of "motivated offender" has often been overlooked in the research, and its concept is not clearly defined. The vast majority of studies have focused on the "suitable targets" and the "absence of guardians"¹⁶ (Bernburg & Thorlindsson, 2001) and assumed that criminal motivation is universal. Furthermore, there is a common belief that "motivated offenders" refer to individuals who already possess pre-existing criminal motivations. However, it is not clearly stated whether those who originally have no criminal intentions, but may be motivated to commit crimes due to specific inducements, also fall under what Cohen and Felson consider the category of motivated offenders. If they do, this indicates that in certain situations, everyone has the possibility of becoming a motivated offender. Therefore, this factor loses its classified function. Besides, RAT would struggle to independently explain such cases¹⁷ (Tillyer & Eck, 2011). It must be combined with other theories (eg. Social Control Theory, Rational Choice Theory, etc.) for analysis in order to adequately obtain valid conclusions in empirical research.

Thirdly, there is a lack of direct methods to measure the three factors of RAT. Researchers often infer these factors through indirect measurements or assumptions. Miethe et al.¹⁸ (1987) also observed that independent tests of lifestyle are absent from the majority of RAT studies, instead using assumed demographic correlates as substitutes. For instance, few studies measuring criminal motivation have substituted neighborhood crime rates for motivated offenders¹⁹ (Massey et al., 1989). In the study by Smith et al.²⁰ (2000), they inferred motivated offenders by indirectly measuring racial structure and distance to central cities, inferred suitable targets by the number of stores, and inferred guardians by the number of houses.

Finally, with the development of the theory, the scope of routine activities becomes difficult to define. Research on RAT seldom considers whether activities that make one more susceptible to victimization are deviant behaviors²¹ (Jensen & Brownfield, 1986). Even the act of engaging in illegal behavior itself can be categorized as a routine activity²² (Mustaine & Tewksbury, 1998). Cohen and Felson² (1979) define routine activities as any recurrent and prevalent activities that fulfill basic population and individual needs. Jensen and Brownfield²¹ (1986) pointed that the activities which are most strongly linked to teenagers being victims of crime are not typical routine activities, such as shopping or dating, but criminal behaviors themselves. Offenders because of their lifestyle and social circles, are more frequently exposed to high-risk situations, thus increasing their likelihood of becoming targets of other criminal acts. Therefore, individuals who engage in criminal activities have a higher likelihood of being victimized by crime. Criminal behavior clearly doesn't satisfy Cohen and Felson's definition of routine activities.

4 Cyber Violence in China

In July 2022, Zheng Linghua was admitted to a famous university. She took a photo with her grandfather holding the admission notice, and shared it on social media to

commemorate the occasion. The next day, she found that her photo was being maliciously spread, and due to her pink hair, the comments insulted her as an escort girl, a nightclub dancer, etc. As a result of cyber violence, she fell into depression and passed away in 2023²³ (Zhang, 2023).

4.1 Motivated Offenders

In 2022, the internet popularizing rate among minors in China reached 97.2%. The proportion of internet users with a bachelor's degree or higher was 9.3%, and those with a monthly income of more than 5000 yuan accounted for 29.3% ²⁴(CNNIC, 2023). Sun and Hao²⁵ (2023) analyzed cyber violence under the framework of RAT. Firstly, they found that these groups of netizens with low education, low income, and underage have relatively weak self-control abilities. They are more likely to be emotionally affected by internet public opinion, and when facing online hot topics or sensitive issues, they are prone to spread information without thinking, or even vent their inner dissatisfaction and anger. The existence of such a large group increases the risk of forming motivations for cyber violence. Secondly, online anonymity is one of the significant reasons behind the motivation for cyber violence^{26,27} (Farrall, & Herold, 2011; Wagner, 2019). Although China has implemented a real-name system on the internet, online identities still retain a feature of front-stage anonymity. When anonymous, netizens' sense of shame and moral views are hidden, making it easier to vent emotions that are constrained in real life through means such as insults, defamation, spreading rumors, and doxxing as forms of cyber violence. Anonymity weakens the participants' sense of guilt, as they do not have to worry about legal or moral repercussions. Therefore, they commit cyber violence against Zheng without any hesitation.

Although their explanations are reasonable, RAT does not play a role in explanation. The former is explained according to Self Control Theory. The less self-control a person has, the more likely he is to commit crimes. The latter reflects the perspective of Rational Choice Theory. Offenders weigh the benefits of their actions against the potential punishments before committing illegal acts. Anonymity reduces the possibility of punishment, making the "benefits" of cyber violence outweigh the "costs". Therefore, RAT cannot explain why people develop criminal motivations, it only states that motivated offenders are generally present. The focus of this theory is on the victim rather than the offender.

4.2 Suitable Targets

Lee²⁸(2022) suggests that the more frequently a person uses the internet, the more likely they are to become victims of cybercrime because they are more exposed to motivated offenders. Firstly, Zheng's inadvertent display of her information might inadvertently provide opportunities for others to commit cyber violence. Many social media platforms and apps allow users to fill out personal profiles, where they can showcase photos of their daily lives and work. Just by piecing together this publicly available information, one can easily gather personal data about individuals without resorting to illegal means or purchasing it.

Secondly, a high degree of online socialization also makes some people primary targets for cyber violence. Zheng is accustomed to sharing her daily life and expressing all kinds of opinions on platforms. She as a blogger has attracted a certain number of fans. The various information and opinions she posts online can often spread and be discussed widely in a short period of time. In China, incidents of internet violence are frequent. A comment made by a netizen may be taken out of context and misinterpreted, which can cause the victim continuous annoyance and irritation^{29,30} (MacFarlane & Bocij, 2003; Lo Moro et al., 2023) such as insults, personal attacks and even cyber manhunt. There have been multiple incidents in China where cyber violence has led to suicide, Zheng is a typical example³¹ (Xu, 2023).

Finally, people who are unwilling to resist are more likely to become the biggest victims. The traditional Chinese culture has always emphasized "harmony is priceless" and "endurance and tolerance". As a well-educated student, Zheng was also influenced by this mindset. She may believe that confronting cyber violence directly is unwise, so she chooses to suffer in silence, such as not responding to the bully's messages and quietly enduring the harm. When some offenders see that the victims do not fight back, they intensify their actions. Some people seeing this situation, will also imitate them³² (Wortley, 2016). This has also led to the phenomenon of "broken windows", with more people engaging in cyber violence, and more people becoming victims.

4.3 Absence of Regulation

Firstly, in China, online platforms often struggle to take effective measures in a timely and active manner, leading to lax supervision. For example, they are slow to respond to victims' complaints, and measures such as deleting illegal posts or banning accounts fail to have a deterrent effect. Additionally, the inaction of some platforms has objectively allowed cyber violence to increase. Zheng's news was very popular at that time. In the intense competition for online traffic, some platforms frequently relax monitoring of the truthfulness and legality of information, allowing illegal and false information to spread unchecked²⁵ (Sun & Hao, 2023). This is because such information can often attract a great deal of attention in a short period, bringing considerable benefits to the platforms.

Secondly, China's current laws on regulating cyber violence are not yet comprehensive enough. Although existing laws have principled provisions against defamation and insult, they do not adequately consider the unique aspects of cyberspace, and their operability and specificity need to be strengthened^{33,34} (Rusakova et al., 2021; Guo, 2024). Besides, from the perspective of the law enforcement, they often face challenges such as insufficient evidence and difficulty in classification when dealing with cases of cyber violence. The legal gaps and delays have resulted in a lack of strong institutional guarantees for combating cyber violence. From the perspective of the victims such as Zheng, they face high costs in defending their rights, and the litigation process is lengthy and complex. They need to invest a great deal of time and money to collect evidence and hire lawyers, while also facing issues such as insufficient evidence and difficulties in evidence collection. As a student, it's hard for Zheng to bear these bur-

dens. Meanwhile, the mental injury caused by cyber violence to victims is often difficult to quantify, and the compensation obtained is rarely commensurate with the cost of defending their rights. In reality, cases that can be resolved through litigation are rare³⁵ (Lin, 2023).

5 Conclusion

RAT can relatively well explain the phenomenon of cyber violence in China. Firstly, netizens excessively expose personal information, making their personal details, life statuses, and preferences easily accessible to others, turning them into targets of cyber violence. For instance, Zheng Linghua shared a photo of her admission to a prestigious school on social media, only to face personal attacks and abuse. Secondly, some netizens are deeply involved in an intense online social life, posting their feelings and views, making their actions easily spark discussions and criticism, and thus becoming targets of cyber violence. Moreover, traditional Chinese culture values make many victims prefer to suffer in silence rather than confront cyber violence directly, which only emboldens bullies and attracts more people to join the abuse, creating a "broken windows" phenomenon. However, RAT does not explain why offenders are motivated to engage in cyber violence. It needs to be combined with other theories, such as the self-control theory, which explains that some people are easily angered by online content due to poor self-control, and rational choice theory, which explains that offenders engage in cyber violence because online anonymity reduces the risk of punishment. Additionally, the lack of governance over illegal content by online platforms and the inadequate operability and specificity of laws and regulations in cyberspace objectively exacerbate the spread of cyber violence. For example, some platforms allow the unchecked spread of false and illegal information to generate web traffic. Moreover, current laws are vague regarding the penalties for online personal harm, and law enforcement faces many difficulties in evidence collection and case qualification, while the legal process for claiming rights is complicated and lengthy, failing to effectively protect the legitimate rights of victims. Therefore, strengthening network supervision is key to curbing cyber violence.

References

1. Sherman, L. W., Gartin, P. R., & Buerger, M. E. (1989). Hot spots of predatory crime: Routine activities and the criminology of place. *Criminology*, 27(1), 27-56.
2. Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 44(4), 588-608.
3. Sun, L., Zhang, G., Zhao, D., Ji, L., Gu, H., Sun, L., & Li, X. (2022). Explore the correlation between environmental factors and the spatial distribution of property crime. *ISPRS International Journal of Geo-Information*, 11(8), 428.
4. Jing, L. J., & Hu, J. (2021). The path to perfecting legal regulations against cyber violence. *Journal of Chinese People's Public Security University (Social Sciences Edition)*, 37(5), 142-149.

5. Kennedy, L. W., & Forde, D. R. (1990). Routine activities and crime: An analysis of victimization in Canada. *Criminology*, 28(1), 137-152.
6. AlKheder, S., Alkandriy, F., Alkhames, Z., Habeeb, M., Alenezi, R., & Al Kader, A. (2022). Walkability, risk perception and safety assessment among urban college pedestrians in Kuwait. *Transportation research part F: traffic psychology and behaviour*, 86, 10-32.
7. Newman, O. (1973). *Defensible space: Crime prevention through urban design*. New York: Collier Books.
8. Perkins, D. D., Florin, P., Rich, R. C., Wandersman, A., & Chavis, D. M. (1990). Participation and the social and physical environment of residential blocks: Crime and community context. *American Journal of Community Psychology*, 18, 83-115.
9. Griffiths, C. T., Dandurand, Y., & Murdoch, D. (2007). *The social reintegration of offenders and crime prevention* (Vol. 4). Ottawa, Ontario, Canada: National Crime Prevention Centre.
10. Webster, C. (2023). Poor Crime: Economic, Welfare and Policy Cycles. In *Rich Crime, Poor Crime: Inequality and the Rule of Law* (pp. 187-204). Emerald Publishing Limited.
11. Moriarty, L. J., & Williams, J. E. (1996). Examining the relationship between routine activities theory and social disorganization: An analysis of property crime victimization. *American Journal of Criminal Justice*, 21, 43-59.
12. Marcum, C. D. (2011). Adolescent online victimization and constructs of routine activities theory. *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*, 253-276.
13. Gottschalk, P. (2019). Organizational convenience for white-collar crime: Opportunity expansion by offender behavior. *Criminal Justice Studies*, 32(1), 50-60.
14. Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. *Internet Research*, 30(6), 1665-1687.
15. de Jong, E., Bernasco, W., & Lammers, M. (2020). Situational correlates of adolescent substance use: An improved test of the routine activity theory of deviant behavior. *Journal of Quantitative Criminology*, 36, 823-850.
16. Bernburg, J. G., & Thorlindsson, T. (2001). Routine activities in social context: A closer look at the role of opportunity in deviant behavior. *Justice Quarterly*, 18(3), 543-567.
17. Tillyer, M. S., & Eck, J. E. (2011). Getting a handle on crime: A further extension of routine activities theory. *Security Journal*, 24, 179-193.
18. Miethe, T. D., Stafford, M. C., & Long, J. S. (1987). Social differentiation in criminal victimization: A test of routine activities/lifestyle theories. *American Sociological Review*, 184-194.
19. Massey, J. L., Krohn, M. D., & Bonati, L. M. (1989). Property crime and the routine activities of individuals. *Journal of Research in Crime and Delinquency*, 26(4), 378-400.
20. Smith, W. R., Frazee, S. G., & Davison, E. L. (2000). Furthering the integration of routine activity and social disorganization theories: Small units of analysis and the study of street robbery as a diffusion process. *Criminology*, 38(2), 489-524.
21. Jensen, G. F., & Brownfield, D. (1986). Gender, lifestyles, and victimization: Beyond routine activity. *Violence and Victims*, 1(2), 85-99.
22. Mustaine, E. E., & Tewksbury, R. (1998). Predicting risks of larceny theft victimization: A routine activity analysis using refined lifestyle measures. *Criminology*, 36(4), 829-858.
23. Zhang, Y. (2023, February 24). *24-year-old pink-haired girl called Zheng Linghua passed away after being cyber violence*. BJD News. <https://baijiahao.baidu.com/s?id=1758694066902088802&wfr=spider&for=pc>
24. China Internet Network Information Center. (2023). *53rd Statistical Report on Internet Development in China*. <https://www.cnnic.cn/n4/2024/0322/c88-10964.html>

25. Sun, Y. H., & Hao, G. K. (2023). Exploration of cyber violence governance strategies from the perspective of routine activity theory. *Journal of Jiangsu Police Institute*, 38(4), 98-106.
26. Farrall, K., & Herold, D. K. (2011). Identity vs. anonymity: Chinese netizens and questions of identifiability. In *Online Society in China* (pp. 165-183). Routledge.
27. Wagner, A. (2019). E-victimization and e-predation theory as the dominant aggressive communication: the case of cyber bullying. *Social Semiotics*, 29(3), 303-318.
28. Lee, C. S. (2022). Online fraud victimization in China: A case study of Baidu Tieba. In *The New Technology of Financial Crime* (pp. 62-81). Routledge.
29. MacFarlane, L., & Bocij, P. (2003). An exploration of predatory behaviour in cyberspace: Towards a typology of cyberstalkers. *First Monday*, 8(9).
30. Lo Moro, G., Scaiola, G., Martella, M., Pagani, A., Colli, G., Bert, F., & Siliquini, R. (2023). Exploring cyberaggression and mental health consequences among adults: An Italian nationwide cross-sectional study. *International journal of environmental research and public health*, 20(4), 3224.
31. Xu Y. Z. (2023, February 21). *Focus on "Cyber Violence Suicides": a review of the tragic suicides caused by cyber violence in recent years*. Upstream News. <https://baijia-hao.baidu.com/s?id=1758405163048000273&wfr=spider&for=pc>
32. Wortley, R. (2016). Situational precipitators of crime. In *Environmental Criminology and Crime Analysis* (pp. 81-105). Routledge.
33. Rusakova, E. P., Inshakova, A. O., & Frolova, E. E. (2021). Legal regulation of internet courts in China. In *Modern Global Economic System: Evolutional Development vs. Revolutionary Leap 11* (pp. 1515-1521). Springer International Publishing.
34. Guo, Z. L. (2024, March 7). *The key to governing cyber violence: focus on the rights and relief of the victims*. ThePaper. https://www.thepaper.cn/newsDetail_forward_26587293
35. Lin, L. (2023, June 10). *Why is it so difficult for ordinary people to defend their rights against cyber violence?* Observer Network. <https://baijia-hao.baidu.com/s?id=1768274853820957128&wfr=spider&for=pc>

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

