The Causes and Measures of Online Deviance

Zhitong Zhao *

Shanghai United International School Hefei Campus, Anhui, China

* Corresponding author: info.hf@suis.com.cn

Abstract. The Internet as a virtual space facilitates the phenomenon of people's deviant behavior. Due to its enormous scale and versatility, it plays an indispensable role in modern society. It is important to maintain online environment and cybersecurity is now a major challenge to society and traditional law enforcement. How is the Internet fueled deviant behavior? What's the difficulties of dealing with online deviance? How to implement intervention without damaging the benefits from the network? This study explains the causes of virtual deviance and gives measures, through the nature of the Internet to answer these questions. Online deviance is influenced by factors like online disinhibition, including benign and toxic disinhibition, which can lead to aggressive behavior due to the absence of immediate feedback. The Internet's characteristics, such as dissociative anonymity and minimized status and authority, worsen online disinhibition, resulting in behaviors like online harassment. Low costs and lenient enforcement contribute to the proliferation of online deviance. Accessible tools and tutorials for cyber deviance, along with online anonymity, further encourage such behavior, creating a self-perpetuating cycle. Defining online deviance is challenging due to its global nature and constantly evolving forms. Laws and definitions vary among countries, and the anonymous nature of online activities hampers identification and classification. Gathering evidence for cyber deviance cases is also complex, as electronic evidence can be tampered with or deleted. It suggests that law enforcement should pay more attention to deal with the reports from Internet users, by implementing targeted warnings and cautions in real world to stop potential criminals, as well as help potential victims be more effective in defending their rights. It also mentions an intervention from family regulatory layer can protect adolescents against deviant behavior from online community. The ideal control effect may be expected to differ, depends on local agencies' capacity and different online policies. This study aims to elucidate the phenomenon of virtual deviance and provide feasible methods to improve online environment. The problems in online society need to be taken seriously.

Keywords: Cyberspace, deviant behavior, cybercrime, targeted warnings.

1. Introduction

As the Internet has evolved over time, it has become an integral part of economic, political, and personal communication due to its vast reach and versatility. Undoubtedly, it now stands as a parallel society alongside the physical world, giving rise to an inevitable concern: cybersecurity. Since the Internet's widespread adoption, online deviant behavior has emerged as a significant challenge for both organizations and individuals, exerting varying degrees of impact on their operations and psychological well-being. The reduction of online deviance, including cybercrime, is pivotal for enhancing societal well-being. Numerous scholars have voiced their concerns about the growing threat posed by cybercrime. The most effective means of combating this threat is through the implementation of stringent legal measures and advanced technological safeguards [1]. Currently, the most pressing issue with cybercrime is not the hypothetical potential for it to someday endanger society as a whole, but rather its pervasive infiltration into people's daily lives.

Common manifestations of online deviance encompass online harassment, cyberaggression, online gossip, and online fraud. Many individuals have personally experienced these transgressions online. According to a 2023 study published by Legal Daily, 61.8 % of 3,591 Internet users reported experiencing online violence and harassment, with 13.4 % indicating severe victimization. The study also examined the consequences of online violence, revealing that 65.0% of victims suffered psychological harm, 59.2% believed that such deviant behavior degraded the online environment, 55.4% felt it propagated negative values and violated moral standards, 35.4% believed it seriously

disrupted victims' daily lives, and 23.0% considered it a breach of privacy and property. Tragically, 9.8% of cases resulted in severe depression and suicide, while 1.4% led to other adverse outcomes. The pervasiveness of online deviance is undeniable, and its harm to individuals is evident. Nevertheless, the unique attributes of cyberspace enable online deviance to persist. This study delves into the root causes of network deviant behavior and proposes corresponding countermeasures.

The Internet, being a virtual realm offering great opportunities and benefits at minimal risk and cost, has led to the prevalence of cybercrime and deviant behavior among netizens. However, the impact of cybercrimes is often less dramatic than anticipated, primarily involving small-scale incidents but affecting multiple victims [2]. While there has been increased attention to online deviance in recent years, exemplified by California's 2022 law allowing users to sue perpetrators of "cyberslacking" without consent, many other smaller deviant acts go underreported and are challenging to address effectively. This is partly because online deviance is not treated with the seriousness it deserves, and much of cybercrime is often viewed through the lens of traditional crime, necessitating law enforcement to approach cybercrime as generalized offenses. This situation undoubtedly hampers law enforcement efficiency and undermines the online environment. Traditional preventive measures have proven ineffective in reducing cybercrime rates, posing the question of how to combat cybercrime more effectively without compromising the inherent benefits of the Internet itself.

This article asserts that the focus of efforts should shift towards addressing online deviant behavior, even when it does not explicitly threaten personal safety or property, such as cases of harassment. While a high frequency of deviant behavior does not necessarily lead directly to criminal acts, it contributes to creating an environment ripe for criminal activities. The Internet, often referred to as "the second society," requires intervention methods tailored to its unique nature. Moreover, these methods must be integrated with real-world actions to achieve meaningful improvements effectively.

2. Causes of online deviant behavior

2.1. Online disinhibition

The nature of the Internet fosters a phenomenon known as online disinhibition, which facilitates deviant behavior more readily than in the offline world. Drawing from the author's extensive literature review, John Suler has distinguished two key categories of online disinhibition: benign disinhibition and toxic disinhibition [3]. In cases of benign disinhibition, the online environment encourages individuals to share personal information and emotions, enabling them to explore their inner selves. Toxic disinhibition, on the other hand, reveals a darker aspect, as it reflects the tendency for some individuals to display aggressive expressions that are seldom used in face-to-face interactions but are easily expressed online, often leading to unintended offenses due to the absence of immediate facial cues and emotional feedback. While the Internet has granted users unprecedented freedom of expression, it is important to note that the majority of netizens do not abandon their moral compass when entering cyberspace, contrary to what is sometimes suggested by media coverage [4]. Toxic disinhibition among netizens often manifests as a transformation of values into harsh judgments and offensive language.

From a different perspective, Suler has identified six commonly studied attributes of online disinhibition, which are closely related to the Internet's unique characteristics: dissociative anonymity, invisibility, asynchronicity, solipsistic introjections, dissociative imagination, and the minimization of status and authority. Furthermore, past research conducted by Christy M.K. Cheung and others has revealed a significant positive correlation between online disinhibition and online harassment [5].

2.2. Low online deviance costs

Reduced costs associated with online deviant behavior can indeed contribute to an escalation in the prevalence of such activities. This perspective has garnered significant attention and research within the realm of network security. When the costs associated with online deviance are minimal,

be it due to lax enforcement of legal regulations or lenient penalties, individuals with malicious intent feel emboldened to engage in such behavior. They may perceive that the consequences of criminal liability would be relatively mild if they were to get caught, diminishing their apprehensions and incentivizing further engagement in online deviant actions.

Moreover, the availability of low-cost avenues for online deviance can also impact individuals' psychological inhibitions. People often grapple with moral and legal dilemmas when contemplating unethical or illegal actions. However, when the costs associated with these actions are low, individuals are more inclined to disregard ethical and legal considerations, as the allure of minimal risk becomes more enticing.

The accessibility afforded by modern technology has facilitated the ease of participation in online deviant behavior. Many malicious actors can acquire the necessary skills through readily available tools and tutorials. Furthermore, the cloak of anonymity afforded by the online environment makes it less cumbersome for them to avoid detection and identification, thereby reducing the likelihood of facing consequences.

Lastly, the presence of low-cost cyber deviance can perpetuate a destructive cycle. As deviant behavior becomes more widespread, cybercrime becomes increasingly prevalent. This, in turn, may lead to a further reduction in costs, as law enforcement agencies may struggle to effectively respond to large-scale cybercrime incidents. This, unfortunately, allows cyberdeviant behavior to continue proliferating.

In summary, the reduced costs associated with online deviance not only encourage more individuals to partake in such activities but also erode moral and legal inhibitions, ultimately fostering a self-perpetuating cycle of cyber deviance and crime.

2.3. Difficulty in determining online deviance

The Internet is a global phenomenon, and online deviant behaviors often span across multiple countries and regions. This global nature of the Internet means that laws and definitions related to cyber breaches can vary significantly from one country to another, leading to challenges in precisely defining what constitutes a cyber breach. What might be considered illegal in one country could be entirely legal in another. Moreover, as network technology continually evolves, new forms of online deviant behavior constantly emerge. Legislators must keep pace with these developments by updating laws to address these novel forms of online misconduct. However, the process of enacting and amending laws is often time-consuming, resulting in a situation where the law lags behind the rapid evolution of technology. This time gap further complicates the task of defining cyber breaches effectively.

The inherent anonymity and disguise provided by the Internet pose another hurdle in defining violations. Many online activities can be carried out anonymously, allowing criminals to conceal their identity and location, thus making it increasingly challenging to track and classify online crimes accurately. Finally, certain forms of online deviance may lack a clearly identified victim, or the victim may not even be aware that they have fallen victim to an online breach. This complexity further muddles the process of defining and monitoring online deviant behaviors. In light of these intricate challenges, it becomes evident that defining and addressing cyber breaches in the ever-evolving online landscape requires a nuanced and adaptive approach, recognizing the global context, the swift pace of technological change, the anonymity factor, and the often-elusive nature of victims in this digital realm.

3. Difficulties of dealing with online deviance

Online deviant behavior often encompasses a range of social and psychological factors, including cyberbullying, online fraud, and online defamation. These behaviors frequently intertwine with psychological issues, adding layers of complexity to the processing of such cases. Furthermore, the virtual world often fosters a sense of detachment and apathy, which can hinder deviants from fully

comprehending the consequences of their actions and impede efforts to reform their behavior. In addition to these challenges, gathering valid evidence in cases of cyber deviance is often more arduous compared to traditional crimes. Electronic evidence is susceptible to tampering, deletion, or concealment, and its preservation often relies on third-party service providers, necessitating legal proceedings for acquisition. These legal processes can be time-consuming and may be subject to international laws, leading to significant delays in case resolution.

The inherently borderless nature of the online realm poses another significant hurdle when addressing online deviance. Given the global reach of the internet, criminals can easily engage in cross-border activities of an international scale. This cross-border complexity complicates coordination and cooperation among different countries, as legal frameworks and law enforcement agencies may vary, making it challenging to consistently combat transnational cyber deviance. Cyber deviant behavior frequently involves highly sophisticated technology and computer knowledge. Hackers and cybercriminals adeptly exploit advanced technological tools to evade detection and tracking, necessitating law enforcement agencies to possess the technical expertise to effectively address these issues. Moreover, the ever-evolving landscape of technology introduces new methods of network deviance, making the fight against cybercrime an ongoing challenge.

Balancing the imperative to protect individual privacy with the necessity of ensuring public safety is another crucial consideration in tackling online deviance. The detection and monitoring of online activities can encroach upon personal privacy, raising ethical and compliance concerns. Consequently, law enforcement agencies must rigorously adhere to established laws and policies to safeguard the rights of innocent individuals during the investigation of online deviance cases. Effectively addressing cyber deviance demands significant resources, encompassing human capital, technical capabilities, and financial investments. Law enforcement agencies often grapple with managing a substantial volume of cybercrime cases with limited resources, which can lead to inefficiencies and case backlogs. Furthermore, certain cybercrimes may be exceptionally complex and international in scope, necessitating large-scale coordination and cooperation, further intensifying resource pressures.

4. Methods of intervention

Deviant ideas generated by the toxic disinhibition stemming from the characteristics of online networks can be challenging to control. However, the occurrence of such behaviors can be mitigated by increasing the costs associated with offensive actions. Among the six characteristics that contribute to network disinhibition, the minimization of status and authority is a significant factor. Timely and targeted warnings from authorities following the identification of deviant behavior can play a crucial role in curbing such activities. These warnings are intended to inform potential wrongdoers about the forthcoming consequences of their actions, ultimately preventing more severe deviant behavior in the future [9]. As rational decision-makers, former offenders are likely to cease their actions when directly deterred. This hypothesis aligns with the deterrence perspective, which can be traced back to principles proposed by Beccaria [10].

To ensure the mature and effective protection of users' rights, a new law enforcement process for reporting network users and implementing countermeasures needs to be established. Technological advancements are reshaping the value of communicative and technical resources, particularly within relevant agencies, as they institutionalize accountability through internal reporting models and procedures. These changes are also restructuring the standard protocols and methods of operational policing [11].

Encouraging collaboration among various network platforms can be beneficial. This cooperation can help address issues such as small-scale but moderately complex fraud cases. By enhancing user security and improving the overall online environment, we can show greater attention and improve efficiency. Consequently, we may see an increase in reported "crimes" driven by malicious intent. In such cases, warnings should also be issued to these users. Police intervention should go beyond merely providing consistent tips to users who download malicious software. It should involve a

stronger direct response to reports that individuals or platforms fail to address promptly. This response may include sending manual email warnings, notifying individuals that their offending behavior has been noticed, and warning of potential legal consequences if they continue their actions. In extreme cases, offline cooperation may be necessary to deter potential criminals who have not yet reached the criminal level. However, it is crucial to avoid improper accusations, as stigmatization can potentially lead to further criminal activity [12].

Intervening in deviant behavior that targets adolescents involves replicating a real-life supervisory layer to some extent. One of the significant differences between the online world and the real world is the diminished or absent role of family supervision. Despite age restrictions on online platforms, a significant number of minors report visiting social networking sites daily. One proposed solution to curbing deviant behaviors against adolescents is to provide common social platforms with a standardized procedure allowing parents to intervene, especially for minors under the age of 14. This approach aims to offer minors maximum psychological and physical protection while minimally limiting their access to the internet.

5. Conclusion

Issues of cybersecurity is a major challenge to modern society, like the deviance occurs in real life, it won't be solved completely, However, forming a method with a combination of traditional crime control measures and technological countermeasures can keep cybercrime within manageable limits. An unhealthy online environment is shaped from the rampancy of all big and small bad phenomena in daily experience, and a high frequency of deviant behavior does not lead directly to crime, but it contributes to shaping an environment where the possibility of crimes is high. It needs to be paid more attention to maintain. Due to the nature of the Internet, online disinhibition provides opportunities for people to do deviant behavior with lower cost compared to in reality. The intervention of virtual deviance should be treated seriously than ever and they need to cope with the nature of the Internet. Currently, the agencies as well as the netizens should try to deal with those small-impact deviance better, by improving the responses in reports from Internet users, giving potential criminals authority cautions, targeted warnings and actual punishments like restriction of virtual liberty in certain situations; setting more feasible protection for minors online; and improving people's awareness of online deviance. What's more, the prevention of cybercrime should not be treated independently of traditional crime. With the continuously updating technology, the threat of cyber deviance will be worse. It is important to shift the focus to cybersecurity by now, and online deviant behavior should be taken seriously by everyone. To further discussion, in order to achieve the results in improving the network environment, these methods need more investigation and practice.

References

[1] Speer D. L. Redefining borders: The challenges of cybercrime. Crime, law and social change, 2000, 34: 259 - 273.

[2] Wall D. S. Cyberspace crime. Routledge, 2017.

[3] Suler J. The online disinhibition effect. Cyberpsychology & behavior, 2004, 7 (3): 321 - 326.

[4] Wall D. S. Cybercrimes and the Internet. Crime and the Internet, 2001, 1 - 17.

[5] Cheung C. M. K., Wong R. Y. M., Chan T. K. H. Online disinhibition: conceptualization, measurement, and implications for online deviant behavior. Industrial Management & Data Systems, 2021, 121 (1): 48 - 64.

[6] Spencer J. Crime on the Internet: Its presentation and representation. The Howard Journal of Criminal Justice, 1999, 38 (3): 241 - 251.

[7] Smahel D, Machackova H, Mascheroni G, et al. EU Kids Online 2020: Survey results from 19 countries. 2020.

[8] Williams M. Virtually criminal: Discourse, deviance and anxiety within virtual communities. Cyberspace Crime. Routledge, 2017, 295 - 304.

[9] Brewer R, de Vel-Palumbo M, Hutchings A, et al. Targeted warnings and police cautions. Cybercrime Prevention: Theory and Applications, 2019: 77 - 90.

[10] Beccaria C. On crimes and punishments. Transaction Publishers, 2016.

[11] Manning P. K. Technology's ways: Information technology, crime analysis and the rationalizing of policing. Cyberspace Crime. Routledge, 2017: 491 - 511.

[12] Becker H. S. Outsiders. Simon and Schuster, 2008.