European Journal of Interdisciplinary Research and Development
Volume- 49 March- 2026
Website: www.ejird.journalspark.org ISSN (E): 2720-5746

NEW FORMS OF SOCIAL RISKS IN THE DIGITAL ENVIRONMENT: CYBER-DEVIATION AND VIRTUAL ANTISOCIAL BEHAVIOR

Mamatnazarov Lazizbek Turakuliyevich
Independent Researcher at the Bukhara State Pedagogical Institute

Abstract
This study examines the emerging constructs of social risk within the digital ecosystem, focusing specifically on cyber-deviation and virtual antisocial behavior. Positioning these phenomena at the intersection of modern deviancology, digital sociology, criminology, and social psychology, the paper systematically analyzes how virtual anonymity, the "space of flows," and deindividuation alter human interaction and weaken traditional social control mechanisms. Applying a comprehensive theoretical framework-including network society theory, general strain theory, social learning theory, differential association, labeling theory, and situational crime prevention-the article establishes a three-tiered taxonomy of digital deviance: virtual asocial behavior, cyber-destructive action (both auto- and hetero-destructive), and virtual antisocial (criminal) conduct. Furthermore, it details the social-economic and moral-ethical ramifications of viral destructive content, moral desensitization, and digital alienation. Ultimately, the study advocates for a balanced strategy combining technological and situational prevention with enhanced digital literacy, digital empathy, and institutional rehabilitation.

Keywords: Digital environment, social risks, cyber-deviation, virtual antisocial behavior, deindividuation, online disinhibition effect, cyberbullying, situational crime prevention, digital empathy.

Introduction

Modern globalization, rapid digitalization, and the deep integration of information and communication technologies into society's lifeworld are fundamentally transforming the traditional architecture of social relations. While the expansion of the information space facilitates socio-economic communications and broadens access to knowledge and resources on one hand, it simultaneously generates new forms of social risks non-inherent to the traditional socium-namely, the phenomena of cyber-deviation and virtual antisocial behavior. Destructive, addictive, and criminal actions emerging within the "space of flows" cause not only the individual-psychological and moral deformation of the personality, but also the functional crisis of social and economic systems, as well as the erosion of society's ethical foundations. Consequently, analyzing the genesis, sociodynamics, and consequences of new forms of social risks in the digital environment from a scientific and methodological perspective stands as one of the most pressing tasks facing modern deviancology, sociology, criminology, and social psychology.

Research Methodology and Approaches (Methods). The conceptualization of deviant behavior within the information society and digital infrastructure finds its expression in the network society theories of M. Castells and M. Poster. The phenomena of anonymity and deindividuation in the digital domain have been investigated by G. Le Bon, E. Diener, and J. Suler. Factors driving cyberbullying and virtual aggression are analyzed through R. Agnew's General Strain Theory and A. Bandura's Social Learning Theory and cognitive modeling framework. The mechanisms governing the dissemination of destructive subcultures and cybercrime are extensively addressed in E. Sutherland's Differential Association Theory and the labeling theory of E. Lemert and H. Becker. Digital models for preventing illegal and hazardous actions draw upon R. Clarke's framework of Situational Crime Prevention.

The primary objective of this article is to conduct a comprehensive scientific and methodological analysis of emerging social risks in the digital environment-specifically the factors driving the formation, taxonomy, and socio-economic as well as moral-ethical consequences of cyber-deviation and virtual antisocial behavior.

Global digitalization, the swift advancement of information and communication technologies, and the deep integration of cyberspace into society's lifeworld are fundamentally transforming the architecture of social relations. While this process streamlines socio-economic communications and expands access to information, it concurrently gives rise to new social risks with distinct geneses-cyber-deviation and virtual antisocial behavior. Evaluating destructive and deviant actions within cyberspace from a scientific and methodological standpoint is a fundamental and complex challenge facing contemporary deviancology, sociology, criminology, and social psychology. To deeply comprehend social risks in the virtual domain, it is first necessary to identify the ontological and sociological characteristics of this environment alongside the trajectories of deviant behavioral models emerging within it.

From a scientific and methodological perspective, analyzing cyber-deviation and virtual antisocial behavior requires relying on the synergy of classical sociological theories and modern digital sociology concepts. As Manuel Castells emphasized in his Network Society theory, information and networked communications forge a new social morphology wherein concepts of power, control, and deviance shift from geographical space to the "space of flows" [1, pp. 185–192]. In the space of flows, the anonymity and networked nature of actions weaken the preventive efficacy of traditional social control institutions (family, community, education, law enforcement). This dynamic aligns with Mark Poster's "Second Media Age" concept; in the digital environment, the individual acquires direct virtual agency and experiences a state of moral-psychological detachment (disembodiment) from the real-world consequences of their actions [2, pp. 104-110].

Anonymity and "deindividuation" play a central role in the formation of cyber-deviation and antisocial behavior in virtual spaces. According to the deindividuation theory developed by G. Le Bon and E. Diener-and later adapted to cyberspace-an individual temporarily loses personal self-identity and internal moral control (self-awareness) when submerged in a crowd or under conditions of virtual anonymity [3, pp. 215–222]. Because the digital realm allows individuals to conceal their name, social status, and physical appearance (via avatars, pseudonyms, and handles), an illusion of freedom from real-world moral taboos and social sanctions takes root.

This leads to what John Suler defined as the "Online Disinhibition Effect" [4, pp. 321–326]. As Suler noted, anonymity and asynchronous communication in digital spaces lay the groundwork for toxic and aggressive impulses to surface.

Results and Analysis (Results). In classifying the degree of social danger and the directional vectors of cyber-deviation and virtual antisocial behavior, it is necessary to differentiate them across three primary models. According to psychological and sociological differentiation, the first form is **virtual asocial behavior**. Here, the individual utilizes the digital information space in an escapist and passively isolated manner. Prominent examples include "digital autism," pathological dependence on virtual life (internet addiction, gaming), nomophobia (fear of being without a mobile device), and "shadow indifference" on social networks. From the standpoint of Alfred Schütz's phenomenological sociology, such individuals withdraw from the everyday lifeworld, lose their social role within virtual subcultures and parallel realities, and adopt an anonymous behavioral strategy [5, pp. 142–148]. While virtual asociality does not inflict direct physical or material harm on others, it leads to the erosion of human capital and social passivity within the individual.

The second form is **cyber-destructive behavior**, distinguished by its orientation toward inflicting harm on either the internal or external environment. In the form of cyber-autodestruction, this manifests through membership in suicidal virtual groups (e.g., games like the "Blue Whale" phenomenon), automutilation, or the spread and promotion of dangerous challenges on social media. In the form of cyber-heterodestruction, it manifests as aggression in digital spaces: cyberbullying (online harassment and insults), hating, cyberstalking, trolling (deliberately disseminating conflictual and negative content), and doxxing (unauthorized publication of private and confidential data). According to Robert Agnew's General Strain Theory, cyberbullying and trolling in virtual environments represent destructive outbursts stemming from emotional frustration and psychological strain (negative emotional states) experienced in real or online life [6, pp. 178–184].

The third, most severe, and socially dangerous level is **virtual antisocial (criminal) behavior**. This form represents an explicit and conscious defiance of constitutional and legal norms, state security, property, and individual dignity. The classification of virtual antisociality encompasses cybercrime (hacking, phishing, theft of banking credentials), operating illicit networks for drugs, weapons, and pornographic content via the Darknet, digital fraud (social engineering), and online recruitment-where extremist, terrorist, and destructive sects ideologically indoctrinate and radicalize youth in virtual spaces. When Edwin Sutherland's Differential Association Theory is applied to digital environments, virtual antisocial and cybercriminal behavior is not biologically inherited; rather, it is acquired by learning destructive techniques and justifying motives within closed Telegram channels, Darknet forums, and cyber-deviant subcultures [7, pp. 156–163].

Discussion

Albert Bandura's Social Learning and Cognitive Modeling Theory holds critical methodological significance in explaining the rapid spread of social risks and cyber-deviations in the digital environment. According to Bandura's model, when individuals displaying

destructive or antisocial behavior in virtual spaces (bloggers, streamers, cyber-popular deviants) attain popularity, monetization, and high social likes, these destructive patterns become imprinted into the cognitive schemes of observers (particularly adolescents and youth) and are replicated en masse [8, pp. 202–208]. The "virality of destructive content" in digital environments leads to the desensitization of deviant behavior-extinguishing moral sensitivity toward destruction and cruelty within society and causing such actions to be perceived as normal.

Another hazardous characteristic of virtual antisocial and cyber-deviant behavior is that it accelerates the process of "secondary deviance" described in Edwin Lemert and Howard Becker's Labeling Theory [9, pp. 134–140]. Individuals labeled as "deviant," "asocial," or "troubled" and marginalized by society and family in real life retreat into the virtual information space to seek self-realization and social support. There, by joining cyber-deviant subcultures, they reinforce their antisocial and destructive identities ("secondary deviance"), executing criminal acts in virtual spaces or via digital tools that they could not carry out in reality.

In modern digital sociology, models of "Situational Crime Prevention" and digital situational intervention are being developed to evaluate and curb the consequences of cyber-deviation and virtual antisocial conduct. According to the situational prevention framework established by Ronald Clarke, it is necessary to reduce anonymity, increase the perceived risk and effort of committing an illicit or destructive act in cyberspace, and decrease the anticipated reward [10, pp. 275–282]. This necessitates early detection and filtering of cyber-destructive content using digital hygiene, biometric identification, artificial intelligence, and algorithmic analysis, alongside establishing situational oversight through "Safe City" and digital neighborhood infrastructures.

At the same time, technical and repressive-legal methods alone cannot eliminate cyber-deviations. Academic analysis indicates that the most priority-driven and humanistic approach to combating virtual antisocial behavior lies in cultivating **media literacy and digital empathy** among the population and youth. It is essential to foster digital hygiene and culture, strengthen ethical norms and netiquette in virtual spaces, and rehabilitate digitally isolated individuals by integrating them into legitimate channels of social mobility.

Conclusion

New forms of social risks in the digital environment-cyber-deviation and virtual antisocial behavior-represent the digital transformation of traditional deviances, possessing a complex, multi-tiered, and dynamic nature. Developing effective prevention mechanisms against these destructive models serves as an essential methodological foundation for ensuring ontological security in society and moral stability across the information space.

References

1. Кастельс М. Информационная эпоха: экономика, общество и культура. – Москва: ГУ ВШЭ, 2000. – С. 185–192.
2. Poster M. The Second Media Age. – Cambridge: Polity Press, 1995. – Pp. 104–110.

3. Diener E. Deindividuation: Causes and Consequences // Social Behavior and Personality. – 1979. – Vol. 7. – No. 2. – Pp. 215–222.
4. Suler J. The Online Disinhibition Effect // CyberPsychology & Behavior. – 2004. – Vol. 7. – No. 3. – Pp. 321–326.
5. Шутц А. Смысловая структура повседневного мира: очерки по феноменологической социологии. – Москва: Институт Фонда «Общественное мнение», 2003. – С. 142–148.
6. Agnew R. Pressured into Crime: An Overview of General Strain Theory. – New York: Oxford University Press, 2006. – Pp. 178–184.
7. Сатерленд Э. Х. Практическое значение теории дифференциальной ассоциации // Социология преступности. – Москва: Прогресс, 1966. – С. 156–163.
8. Бандура А. Теория социального научения. – Санкт-Петербург: Евразия, 2000. – С. 202–208.
9. Лемерт Э. Социальная патология: концепция первичной и вторичной девиации. – Санкт-Петербург: Питер, 2016. – С. 134–140.
10. Clarke R. V. Situational Crime Prevention: Successful Case Studies. – Harrow and Heston, 1997. – Pp. 275–282.