ACADEMIC SCIENCE PRESS

INTERNATIONAL JOURNAL OF SOCIETY, CULTURE AND HUMAN SCIENCES
ISSN: 3143-6463

Organizational and Legal Mechanisms for Improving the Prevention of Deviant Behavior in the Digital Space and Cyber-Radicalization Among young people

Akhmetova Nodira Orifovna [1]
[1] Independent researcher

ARTICLE INFO

Keywords:
digital space,
deviant behavior,
cyber-radicalization,
extremism,
youth,
prevention,
media literacy,
inoculation theory,
cyberbullying,
counter-narrative.

Vol. 01, **No**. 05, 2026

https://doi.org/10.5281/zenodo.23231978

Copyright © 2026 by author(s) and Scientific Research Publishing Inc. This work is licensed under the Creative Commons Attribution International License (CCBY4.0).

http://creativecommons.org/licenses/by/4.0/

Open Access

ABSTRACT

The rapid shift of young people's education, communication and leisure into the digital space has created new risks that traditional institutions of social control – the family, the school and the mahalla – are unable to monitor adequately. Two of these risks are usually studied separately: deviant behavior in the digital space (cyberbullying, trolling, online gambling, participation in self-harm communities and illegal online activity) and cyber-radicalization, i.e. young people falling under the influence of extremist ideology via the Internet. The aim of this article is to substantiate the interrelationship between these two phenomena and to develop organizational and legal proposals for improving their prevention in the Republic of Uzbekistan. The study uses systemic-structural, comparative legal and logical-legal analysis and content analysis of the academic literature, national legislation and the approaches of the European Union, the United Kingdom and Finland. The results show that digital deviance and cyber-radicalization share common determinants – personal vulnerability, the online disinhibition effect and the primacy of closed-group norms – and that the first two of the five identified stages of cyber-radicalization (vulnerability and exposure) largely coincide with the risk factors for digital deviance. Five gaps in national legislation are identified, including the absence of a legal definition of cyberbullying, of specific forms of preventing offences in the digital space, of platform obligations to protect minors, and of a rehabilitative procedure for young people influenced by radical ideas who have not committed a crime. A three-level prevention model (universal, targeted and individual) is proposed, together with an outcome-based system for evaluating effectiveness. Seven recommendations for improving legislation and practice are formulated, aimed at shifting the prevention system from a reactive and restrictive model to a proactive, targeted and multi-agency one.

Introduction

The rapid development of information and communication technologies has shifted almost every sphere of young people's lives into the digital space. Education, communication, entertainment, professional development and civic engagement are today largely carried out through a smartphone screen. While creating unprecedented opportunities for young people, this has also given rise to new risks that traditional institutions of social control – the family, the school and the mahalla – are unable to monitor adequately.

Among these risks, two interrelated phenomena require particular attention. The first is deviant behavior in the digital space, i.e. cyberbullying, trolling, online gambling, membership in communities promoting self-harm, and involvement in illegal online activity. The second is cyber-radicalization, i.e. young people falling under the influence of extremist ideology via the Internet. In academic literature these two phenomena are often studied separately; however, practice shows that they share common roots and can merge into one another.

In the Republic of Uzbekistan, youth issues are defined as a priority area of state policy. The legal framework in this area comprises the Law "On State Youth Policy" [15], the Law "On the Prevention of Offences" [10], the Law "On Countering Extremism" [11], the Law "On the Protection of Children from

Information Harmful to Their Health" [12], the Law "On Cybersecurity" [13], the National Strategy for Countering Extremism and Terrorism for 2021–2026 approved by Presidential Decree No. PF-6255 [16], and the "Uzbekistan – 2030" Strategy [14]. Nevertheless, the rapidly changing nature of threats in the digital environment calls for continuous improvement of prevention mechanisms.

Literature review

The theory of deviant behavior has a long history in the social sciences. É. Durkheim's concept of anomie, R. Merton's strain theory [27], E. Sutherland's differential association theory and H. Becker's labeling theory explain the social roots of deviance from different perspectives. In the post-Soviet academic tradition, Yu.A. Kleiberg and E.V. Zmanovskaya systematically examined the psychological nature, types and prevention of deviant behavior [1; 2]. These theories remain relevant to the digital space, but they need to be supplemented with an account of the specific features of the digital environment.

J. Suler's concept of the "online disinhibition effect" is the main theoretical basis for explaining changes in behavior in the digital space [3]. Owing to anonymity, invisibility, asynchronicity, solipsistic introjection, dissociative imagination and the minimization of status differences, people behave more freely online than offline. This freedom may manifest itself in positive forms (openness, willingness to help) and negative forms (aggression, insults).

In cyberbullying research, the works of S. Hinduja and J. Patchin hold a leading place [4]. They identified the features that distinguish cyberbullying from traditional bullying – permanence, rapid spread to a wide audience, the anonymity of the aggressor and the defenselessness of the victim – and proposed models of prevention programmes in schools. The meta-analysis by R. Kowalski and co-authors confirmed that cyberbullying victimization is associated with depression, anxiety, loneliness and reduced well-being, while perpetration is associated with normative beliefs about aggression and moral disengagement [20].

Two approaches to cyber-radicalization have emerged in the foreign literature. Proponents of the first regard the Internet as an independent and powerful factor of radicalization: P. Neumann emphasizes that the Internet functions as an "echo chamber", normalizes radical views and accelerates individual radicalization [5]. Representatives of the second, including M. Conway, argue that the role of the Internet should be considered in close connection with offline factors and assessed not as the sole cause of radicalization but as its "catalyst" [6]. The systematic review by G. Hassan and co-authors shows that active seeking of extremist content is associated with radical attitudes, but that this association is mediated by personal characteristics [7]. Process models of radicalization – F. Moghaddam's "staircase to terrorism" [19], R. Borum's review of radicalization theories [17] and C. McCauley and S. Moskalenko's "two-pyramids" model separating radical opinion from radical action [18] – show that radicalization unfolds in stages and that most people holding radical opinions never move to action, which opens a window for prevention.

J.M. Berger defines extremism as the belief that an in-group's success is inseparable from hostile action against an out-group [8]. This definition yields an important practical conclusion: the core of extremist propaganda lies in questions of identity and belonging, and an effective response must likewise satisfy these needs in a positive way. Finally, research on psychological inoculation, going back to W. McGuire [21], has recently demonstrated in large field experiments that short prebunking videos improve young people's ability to recognize manipulation techniques on social media [22].

Uzbek scholars have extensively studied the spiritual education of young people, ideological immunity and resistance to information attacks within philosophy, pedagogy and law. However, a comprehensive study of digital deviance and cyber-radicalization as a single object of prevention has not yet been carried out. This article aims to partially fill this gap.

The purpose of the article is to provide a theoretical substantiation of the interrelationship between deviant behavior in the digital space and cyber-radicalization among young people and to develop organizational and legal proposals aimed at improving their prevention. The research questions are: (1) what common determinants link digital deviance and cyber-radicalization; (2) what gaps exist in the national organizational and legal framework of prevention; (3) what lessons can be drawn from foreign experience; and (4) what prevention model is appropriate for Uzbekistan.

Materials and methods

The material of the study comprised national legislation in its current wording [10–16], the Criminal Code of the Republic of Uzbekistan, foreign legal acts and policy documents – the EU Digital Services Act [9], the European strategy for a better internet for kids (BIK+) [24], the UK Online Safety Act 2023 [23] and the statutory guidance on the Channel programme [25] – and the academic literature on deviance, cyberbullying and radicalization [1–8; 17–22].

The study used the methods of systemic-structural analysis (to identify common determinants and stages), comparative legal analysis (to compare national and foreign mechanisms), logical-legal analysis (to identify gaps in legislation), induction and deduction, and content analysis of the academic literature. The approaches of the European Union, the United Kingdom and Finland were selected for comparison because they represent, respectively, a supranational regulatory approach to platforms, a combined regulatory and multi-agency support approach, and an educational approach based on media literacy. In developing the prevention model, the concept of primary, secondary and tertiary prevention widely used in public health [26] served as the methodological basis.

Results

1. The interrelationship between digital deviance and cyber-radicalization

The analysis shows that deviant behavior in the digital space and cyber-radicalization share a number of common determinants. First, both phenomena are characterized by personal vulnerability factors – social isolation, identity crisis, low self-esteem, a sense of injustice and aggressiveness. Second, in both cases the online disinhibition effect weakens moral restraint mechanisms [3]. Third, in both cases closed online communities place group norms above the norms of the wider society.

Moreover, a trajectory from deviant behavior to radicalization can be observed in practice. A teenager who has been a victim of cyberbullying may feel defenseless and misunderstood by society and fall under the influence of radical groups that promise "protection" and "revenge". Likewise, young people accustomed to trolling and spreading offensive content find it psychologically easier to adopt hate speech and use it within the framework of extremist ideology. For this reason, the prevention of digital deviance is at the same time the early prevention of cyber-radicalization. The differences between the two phenomena are summarized in Table 1.

Table 1

Comparative characteristics of digital deviant behavior and cyber-radicalization

Criterion	Digital deviant behavior	Cyber-radicalization
Main motivation	Self-affirmation, entertainment, emotional release, quick income	Belonging, search for meaning, notions of justice and revenge
Social environment	Peer groups, open platforms	Closed channels, encrypted messengers, recruiters
Risk factors	Impulsivity, weak supervision, anonymity	Identity crisis, isolation, algorithmic "echo chamber"
Consequences	Psychological trauma, offences, addiction	Involvement in extremist activity, criminal liability
Prevention actors	Family, school, psychologist, prevention inspector	All of the above + specialized agencies, religious scholars

Source: developed by the author.

2. Stages of cyber-radicalization

Based on the literature [17–19] and practice, five stages can be distinguished (Table 2).

Table 2

Stages of cyber-radicalization and windows for prevention

Stage	Content	Overlap with digital deviance	Main prevention actors
1. Vulnerability	Identity crisis, isolation, sense of injustice	High	Family, school, mahalla
2. Exposure	Encountering radical resources through seemingly harmless content	High	Family, school, media literacy
3. Recruitment	Recruiters initiate personal contact and invite into closed groups	Partial	Psychologists, youth leaders, platforms
4. Isolation and indoctrination	Distancing from family and friends, "us versus them" worldview	Low	Multidisciplinary team
5. Mobilization	Spreading propaganda, fundraising, other illegal actions	Low	Law enforcement agencies

Source: developed by the author based on [17–19].

The most important finding from the standpoint of prevention is that the first two stages almost entirely coincide with the risk factors for digital deviance. Consequently, it is precisely at these stages that the family, the school and the mahalla have the most effective opportunity to intervene.

New technological trends amplify these risks. First, online gaming platforms and their chat functions have become a convenient venue for establishing direct contact with young people: parental oversight there is weak, and communication takes place under the guise of a "game". Second, short-video formats and recommendation algorithms can "pull" a user into a stream of extreme content within minutes. Third, deepfakes created with artificial intelligence tools and disinformation spread by

automated accounts erode trust in the information environment. Fourth, closed channels in encrypted messengers hide communication from external observation.

3. Gaps in the existing organizational and legal mechanisms

National legislation contains several avenues for protecting young people in the digital space. The Law "On the Protection of Children from Information Harmful to Their Health" defines the types of information prohibited from distribution to children [12]. The Law "On Countering Extremism" provides for a procedure for identifying extremist materials and prohibiting their distribution [11]. Article 244¹ of the Criminal Code establishes liability for producing, storing, distributing or displaying materials that threaten public security and public order, including via the Internet. The Law "On the Prevention of Offences" sets out general and special prevention measures and the system of actors responsible for implementing them [10].

At the same time, the analysis identified the following problems: first, the Law "On the Prevention of Offences" does not provide for specific forms and methods of preventing offences committed in the digital space; second, the concept of cyberbullying has no legal definition in national legislation, which makes it difficult to identify and record such cases and to determine response measures; third, a unified mechanism for information exchange and coordination on digital threats among prevention actors (educational institutions, youth affairs bodies, internal affairs bodies, the mahalla) has not been sufficiently developed; fourth, the obligations of digital platforms to protect children and young people from harmful content are not clearly defined; fifth, a rehabilitative and preventive procedure for working with young people who have fallen under the influence of radical ideas but have not committed a crime is insufficiently developed.

The digital competence of prevention actors is a further problem. Many teachers, prevention inspectors and parents lack a sufficient understanding of the platforms young people use, their internal culture, slang and rules of communication. As a result, warning signs go unnoticed or, conversely, harmless situations are unjustifiably assessed as dangerous, undermining trust-based relationships with young people.

4. Foreign experience

In the European Union, Safer Internet Centres operate in each member state under the BIK+ strategy [24]; they combine awareness-raising, helplines for children and parents, and hotlines for reporting illegal content. The Digital Services Act imposes obligations on very large online platforms to assess systemic risks and to ensure a high level of privacy, safety and security of minors [9].

In the United Kingdom, the Online Safety Act 2023 imposes duties of care on platforms to protect children from harmful content and entrusts oversight to an independent regulator [23]. The Channel programme provides for the early identification of individuals susceptible to radicalization and multi-agency, voluntary support for them [25]. Finland's experience is distinguished by the integration of media literacy into lifelong learning starting from preschool education. The main lessons are: sharing responsibility for prevention among the state, the family, the education system and platforms; providing support to at-risk individuals before resorting to punishment; and making media literacy an integral part of lifelong learning.

5. A three-level prevention model

Based on these results, a three-level model for the prevention of digital deviance and cyber-radicalization among young people has been developed (Table 3).

Table 3

Three-level model for the prevention of digital deviance and cyber-radicalization

Level of prevention	Target group	Key measures
Universal (primary)	All children and young people, parents	Media literacy and digital safety courses, "digital parenting" training, positive content with counter-narratives, meaningful leisure activities
Targeted (secondary)	At-risk young people (those involved in cyberbullying, socially isolated, in difficult family circumstances)	Screening by school psychologists, mentoring, group training, helpline and chatbot service, individual follow-up by youth leaders
Individual (tertiary)	Young people with identified deviant or radical behavior	Individual programme delivered by a multidisciplinary team (psychologist, teacher, religious scholar, prevention inspector), rehabilitation and reintegration, family support

Source: developed by the author.

Resources are directed primarily towards universal prevention as the most far-reaching and least costly approach, while targeted and individual prevention focus on risk groups identified on the basis of clear criteria. This eliminates the "one-size-fits-all" character of preventive measures.

Discussion

Interpretation in the light of the literature

The findings support the position of M. Conway and G. Hassan that the Internet acts as a catalyst rather than the sole cause of radicalization [6; 7]: the decisive factors at the initial stages are personal vulnerability and the need for belonging, which are also the roots of digital deviance. At the same time, the role of recommendation algorithms and closed channels described by P. Neumann [5] explains why, once exposure has occurred, the transition through the subsequent stages can be very rapid. The two-pyramids model [18] implies that prevention should not treat every young person with radical opinions as a potential offender; this justifies the separation of universal, targeted and individual levels and the voluntary nature of tertiary measures.

The role of the mahalla

The mahalla is of particular importance in implementing the model. The youth leader, the prevention inspector and the women's activist, who are part of the mahalla "seven", are the actors with the closest knowledge of young people and families. Training them to identify digital threats and coordinating their work with psychologists at educational institutions would significantly increase the effectiveness of prevention. This national institution can play a role similar to the multi-agency panels of the UK Channel programme [25], but with stronger community roots.

Media literacy and counter-narratives

Restrictive measures (blocking content, closing accounts) are necessary but not sufficient: content quickly migrates to new platforms, and excessive bans heighten interest among some young people. Building "ideological immunity", i.e. developing young people's ability to independently recognize and resist manipulation, is therefore a priority. According to inoculation theory, exposing a person in advance to weakened examples of manipulative techniques increases their resistance to subsequent manipulation [21; 22]. It would be advisable to apply this approach widely in media literacy classes. When creating

counter-narratives, credibility is decisive: official-sounding content that does not speak the language of young people fails, while the life stories of bloggers, athletes and artists respected among young people, as well as of people who have left radical groups, are more impactful. This corresponds to Berger's conclusion that effective responses must satisfy the need for identity and belonging [8].

Evaluating the effectiveness of prevention

In practice, effectiveness is often measured by the number of events held and participants. Such indicators do not reflect real changes in behavior. It is proposed to use outcome-oriented indicators: the level of young people's media literacy (pre- and post-intervention tests), the proportion of those who report cases of cyberbullying, the number of requests to support services and the rate at which they are resolved, the proportion of repeat offences among at-risk young people, and parents' awareness of digital risks. Such indicators allow prevention programmes to be improved on an evidence basis.

Limitations

The study is theoretical and comparative-legal; the proposed model and indicators have not yet been tested empirically. The national prevalence of digital deviance and cyber-radicalization among young people is not documented by regular representative surveys, which limits quantitative assessment. Piloting the model in several regions with a pre- and post-evaluation is a direction for further research.

Conclusion

The study led to the following conclusions. First, deviant behavior in the digital space and cyber-radicalization are interrelated phenomena with common determinants, and digital deviance often serves as a "gateway" to radicalization. Second, the current prevention system is predominantly reactive and restrictive and does not fully take into account the specific features of the digital environment. Third, the effectiveness of prevention depends on transitioning to a three-level, targeted and multi-agency model.

Based on the above, the following proposals are put forward:

1. To introduce into the Law "On the Prevention of Offences" a separate article on the prevention of offences in the digital space, providing for measures such as online preventive interviews, digital warnings and online social adaptation.

2. To introduce a legal definition of "cyberbullying" into national legislation and to approve a model procedure for responding to cases of cyberbullying in educational institutions.

3. To create a unified interagency platform for information exchange on digital threats among the Youth Affairs Agency, the Ministry of Preschool and School Education, the Ministry of Higher Education, Science and Innovation, and the Ministry of Internal Affairs.

4. To consider establishing obligations for digital platforms operating in the national segment to protect minors from harmful content (a complaints mechanism, age verification, deadlines for handling complaints).

5. To introduce a voluntary rehabilitation and prevention programme, involving a multidisciplinary team of specialists, for young people who have fallen under the influence of radical ideas but have not committed a crime.

6. To include a media literacy module based on the inoculation approach in the curricula of general secondary schools and higher education institutions.

7. To conduct an annual national sociological survey of digital behavior among young people and to use its results in planning prevention programmes.

The implementation of these proposals will make it possible to raise young people as safe and responsible participants in the digital space, protect them from the influence of deviant behavior and radical ideas, and shift the prevention system from a reactive to a proactive model.

References

1. Kleiberg Yu.A. Psikhologiya deviantnogo povedeniya [Psychology of Deviant Behavior]: textbook. – Moscow: TC Sfera, 2001. – 160 p. (in Russian)
2. Zmanovskaya E.V. Deviantologiya: psikhologiya otklonyayushchegosya povedeniya [Deviantology: The Psychology of Deviant Behavior]. – Moscow: Akademiya, 2003. – 288 p. (in Russian)
3. Suler J. The Online Disinhibition Effect // CyberPsychology & Behavior. – 2004. – Vol. 7, № 3. – P. 321–326.
4. Hinduja S., Patchin J.W. Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying. 2nd ed. – Thousand Oaks: Corwin, 2015. – 312 p.
5. Neumann P.R. Options and Strategies for Countering Online Radicalization in the United States // Studies in Conflict & Terrorism. – 2013. – Vol. 36, № 6. – P. 431–459.
6. Conway M. Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research // Studies in Conflict & Terrorism. – 2017. – Vol. 40, № 1. – P. 77–98.
7. Hassan G., Brouillette-Alarie S., Alava S. et al. Exposure to Extremist Online Content Could Lead to Violent Radicalization: A Systematic Review of Empirical Evidence // International Journal of Developmental Science. – 2018. – Vol. 12, № 1–2. – P. 71–88.
8. Berger J.M. Extremism. – Cambridge, MA: MIT Press, 2018. – 216 p.
9. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act) // Official Journal of the European Union. – L 277. – 27.10.2022.
10. Law of the Republic of Uzbekistan "On the Prevention of Offences". No. ZRU-371 of 14.05.2014.
11. Law of the Republic of Uzbekistan "On Countering Extremism". No. ZRU-489 of 30.07.2018.
12. Law of the Republic of Uzbekistan "On the Protection of Children from Information Harmful to Their Health". No. ZRU-444 of 08.09.2017.
13. Law of the Republic of Uzbekistan "On Cybersecurity". No. ZRU-764 of 15.04.2022.
14. Decree of the President of the Republic of Uzbekistan "On the 'Uzbekistan – 2030' Strategy". No. PF-158 of 11.09.2023.
15. Law of the Republic of Uzbekistan "On State Youth Policy". No. ZRU-406 of 14.09.2016.
16. Decree of the President of the Republic of Uzbekistan "On approval of the National Strategy of the Republic of Uzbekistan for Countering Extremism and Terrorism for 2021–2026". No. PF-6255 of 01.07.2021.
17. Borum R. Radicalization into Violent Extremism I: A Review of Social Science Theories // Journal of Strategic Security. – 2011. – Vol. 4, № 4. – P. 7–36.
18. McCauley C., Moskalenko S. Understanding Political Radicalization: The Two-Pyramids Model // American Psychologist. – 2017. – Vol. 72, № 3. – P. 205–216.
19. Moghaddam F.M. The Staircase to Terrorism: A Psychological Exploration // American Psychologist. – 2005. – Vol. 60, № 2. – P. 161–169.

20. Kowalski R.M., Giumetti G.W., Schroeder A.N., Lattanner M.R. Bullying in the Digital Age: A Critical Review and Meta-Analysis of Cyberbullying Research Among Youth // Psychological Bulletin. – 2014. – Vol. 140, № 4. – P. 1073–1137.

21. McGuire W.J. Inducing Resistance to Persuasion: Some Contemporary Approaches // Advances in Experimental Social Psychology. – 1964. – Vol. 1. – P. 191–229.

22. Roozenbeek J., van der Linden S., Goldberg B., Rathje S., Lewandowsky S. Psychological Inoculation Improves Resilience Against Misinformation on Social Media // Science Advances. – 2022. – Vol. 8, № 34. – eabo6254.

23. Online Safety Act 2023 (c. 50). – London: The Stationery Office, 2023. – URL: https://www.legislation.gov.uk/ukpga/2023/50

24. European Commission. A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+). COM(2022) 212 final. – Brussels, 11.05.2022.

25. HM Government. Channel Duty Guidance: Protecting People Susceptible to Radicalisation. – London: Home Office, 2023.

26. Caplan G. Principles of Preventive Psychiatry. – New York: Basic Books, 1964. – 304 p.

27. Merton R.K. Social Structure and Anomie // American Sociological Review. – 1938. – Vol. 3, № 5. – P. 672–682.