The OSCAR PUBLISHING Services
International Journal of Law And Criminology

VOLUME Vol.05 Issue06 2025
PAGE NO. 72-74
DOI 10.37547/ijlc/Volume05Issue06-15

# Preventive Measures to Combat Cybercrime: A Criminological Perspective (Educational and Social Measures, Work with Youth, Development of Digital Literacy)

Dusmatov Durbek Rustamjon ugli

Tashkent City Prosecutor's Office Prosecutor of the Department in the field of counteraction shadow economy, 2nd class lawyer, Tashkent city, Uzbekistan

**Received:** 30 April 2025; **Accepted:** 28 May 2025; **Published:** 30 June 2025

**Abstract:** In the context of society's digitalization, cybercrime is becoming one of the most pressing threats to public security. This article examines preventive measures to combat cybercrime from a criminological perspective. Special attention is given to educational, social, and cultural strategies aimed at building societal resilience—particularly among youth—against involvement in unlawful online activities.

**Keywords:** Cybercrime, criminology, prevention, prophylaxis, digital literacy, youth, social prevention, legal culture.

**Introduction:** Modern digital technologies, on the one hand, have provided unprecedented opportunities for communication, education, and commerce; on the other hand, they have become instruments for committing new forms of crimes. Cybercrime today constitutes one of the most rapidly evolving threats to public security, necessitating not only criminal law responses but also effective criminological prevention.

According to UN data, cybercrime continues to show steady growth each year. However, traditional preventive methods prove to be ineffective due to the anonymity of cybercriminals, the transnational nature of offenses, and rapid technological advancements. Under these conditions, preventive measures gain critical importance, particularly in the context of youth engagement and enhancing digital literacy among the general population.

The information society, while offering vast opportunities for the development of individuals and states, has simultaneously given rise to new forms of criminality. Cybercrime is marked by high latency, transnationality, and swift evolution. In such circumstances, the criminological approach—focusing on the prevention of crime—becomes particularly significant. Preventive measures aim not only to eliminate conditions conducive to crime but also to foster legal awareness, digital culture, and critical thinking among citizens.

Criminological prevention is grounded in the principles of identifying and eliminating the causes and conditions conducive to crime. Unlike criminal law measures, which are directed at punishing already committed offenses, preventive efforts are aimed at building societal resilience to criminal behavior.

Cybercrime is characterized by several features that demand a specialized preventive approach:

- The decentralized nature of threats;
- The physical detachment of offenders from their targets;
- High levels of technical proficiency among offenders;
- The widespread involvement of youth in cybercriminal activity.

Therefore, cybercrime prevention requires a multidisciplinary approach that integrates legal, pedagogical, sociological, and psychological tools.

**Enhancing digital literacy is a key direction in cybercrime prevention**. Research indicates that groups with higher IT competence and legal awareness exhibit significantly lower rates of engagement in unlawful online activities.

One of the most important preventive measures is the promotion of digital literacy and legal education. Studies show that a low level of knowledge regarding cyber threats and legal liability for online behavior contributes to the rise of offenses, especially among young people.

School and university curricula should include:

- Fundamentals of information security;
- Legal foundations of online behavior;
- Digital communication ethics;
- Skills for identifying fake news, phishing, cyberbullying, and other online risks;
- Inclusion of courses on cybersecurity and digital ethics in school and university programs;
- Training of teachers and academic advisors to identify digital risks;
- Implementation of supplementary educational programs involving IT professionals and legal experts.

Positive examples of such educational initiatives are observed in the European Union through the Digital Education Action Plan, which implements mandatory cybersecurity modules for students.

Similar approaches are also implemented in the domestic initiative “Digital Literacy for All” with the support of the Ministry of Digital Development of the Russian Federation.

Moreover, youth involvement in cybercrime is also driven by social and psychological factors such as the desire for recognition, self-assertion, rebellious attitudes, and a fundamental lack of legal awareness. Therefore, in addition to educational efforts, comprehensive programs of social prevention are required.

Social prevention plays a critical role, aiming to reduce levels of social tension, marginalization, and maladjustment, especially among adolescents. Youth involvement in cybercrime is often motivated not solely by criminal intent but by social immaturity, a desire for recognition, or a lack of understanding of the legal consequences.

Recommended measures include:

- Establishing youth IT clubs, hackathons, and forums on digital ethics;
- Engaging students in ethical hacking and digital volunteer projects;
- Providing psychological support to vulnerable teenagers with deviant behavior;
- Promoting “digital role models” — successful IT specialists, ethical bloggers, and social activists.

**Special attention should be paid to families and educational institutions** as the primary environment for shaping digital values and legal consciousness.

Criminological data show that the majority of cybercrimes are committed by individuals aged 14 to 30, due to both technical aptitude and social insecurity.

Proposed directions for youth engagement:

- Creation of university “cyber patrols” — student organizations monitoring online offenses and promoting lawful behavior;
- Conducting interactive lectures with participation from police, prosecutors, and cyber psychologists;
- Involving youth in digital rights protection activism;
- Implementing gamified legal education methods (quests, simulations, interactive case studies).

This approach aligns with international standards for juvenile crime prevention as outlined in the UN Guidelines for the Prevention of Juvenile Delinquency (“The Riyadh Guidelines”).

**Cybercrime is a multifaceted issue**, and its prevention is only possible through coordinated efforts of the state, businesses, civil society, and academia. Best results are achieved through:

- Creation of interagency councils on digital security;
- Regular public awareness campaigns on cyber threats and protection measures;
- Legal outreach: publications, videos, and social media content.

In Uzbekistan, the National Strategy for Enhancing Digital Literacy and Legal Awareness is already being implemented in cooperation with the UN, OSCE, and UNICEF.

**Thus, preventive measures against cybercrime must be systemic, based on a scientifically grounded criminological strategy with a long-term vision**. Particular emphasis should be placed on youth policy, digital education, and inter-agency coordination. Effective prevention requires not only regulatory mechanisms but also humanitarian efforts aimed at fostering a digital legal culture as a key factor in resilience to cyber threats. In conclusion, it is essential to emphasize that cybercrime prevention policy must be integrative in nature, combining educational, social,

cultural, and legal measures. Youth engagement, development of digital immunity, and moral-legal orientation are central pillars. Only a comprehensive approach grounded in criminological research can ensure a sustainable reduction in cybercrime in the long run.

**REFERENCES**

Shestakov, D.A. Cybercrime: Criminal Law and Criminological Aspects. — St. Petersburg: Legal Center Press, 2021.

Mikhailova, E.A. Digital Literacy as a Factor in Preventing Internet Crime // Criminology: Yesterday, Today, Tomorrow. — 2022. — No. 1. — Pp. 73–80.

European Commission. Digital Education Action Plan (2021–2027). https://education.ec.europa.eu

Chernyshov, I.V. Youth Deviance in the Digital Environment // Youth Sociology. — 2021. — No. 4. — Pp. 52–58.

UNODC. Global Study on Cybercrime. United Nations, 2020.

United Nations. Guidelines for the Prevention of Juvenile Delinquency (The Riyadh Guidelines), 1990.

Ministry of Digital Technologies of the Republic of Uzbekistan. National Program for the Development of Digital Literacy (2022–2026).

UNODC. Global Cybercrime Study. — Vienna: United Nations, 2022.

Kudryavtsev, V.N. General Theory of Crime. — Moscow: Legal Literature, 2020.