

Scientific Perspectives on The Methods of Committing Property Crimes in Cyberspace

 Utaev Khusniddin Khurramovich

Independent Researcher, Tashkent State University of Law, Uzbekistan

Received: 28 Mar 2026 | Received Revised Version: 20 Mar 2026 | Accepted: 04 May 2026 | Published: 31 May 2026

Volume 08 Issue 05 2026 | Crossref DOI: 10.37547/tajpslc/Volume08Issue05-16

Abstract

This article presents scientific perspectives on the methods of committing property crimes in cyberspace. The article analyzes the criminological characteristics of crimes committed in cyberspace in the Republic of Uzbekistan, particularly cyber fraud of a property-related nature, as well as its social danger and issues of criminal liability.

Keywords: Information and communication, information input, crimes, punishment, technologies, cyberspace, property, commission, methods, social danger.

© 2026 Utaev Khusniddin Khurramovich. This work is licensed under a Creative Commons Attribution 4.0 International License (CC BY 4.0). The authors retain copyright and allow others to share, adapt, or redistribute the work with proper attribution.

Cite This Article: Utaev Khusniddin Khurramovich. (2026). Scientific Perspectives on The Methods of Committing Property Crimes in Cyberspace. The American Journal of Political Science Law and Criminology, 8(05), 97–102. <https://doi.org/10.37547/tajpslc/Volume08Issue05-16>

1. Introduction

Fraud has been regarded as a particularly dangerous crime in the majority of countries around the world since ancient times. Uzbekistan is no exception in this regard. Fraud is characterized by its adaptability to changing circumstances, its manifestation in various forms, and its ability to penetrate virtually all spheres of social life.

Particular attention is being paid to strengthening the protection of various forms of property, establishing guarantees for property and property rights, and implementing incentive provisions in law enforcement practice. These provisions include the exemption from criminal liability, on the grounds of reconciliation, of persons who have committed the offense provided for in Part 1 of Article 168 of the Criminal Code of the Republic of Uzbekistan, as well as provisions stipulating that restriction of liberty or imprisonment should not be

imposed where the material damage caused by the offense has been fully compensated. A number of targeted measures are being implemented in this area.

The failure to impose fair and proportionate punishment on persons found guilty of fraud may contribute to their reoffending. Therefore, persons who have committed a crime should be given an appropriate opportunity to prevent them from committing further offenses after serving their punishment.

The lack of trust between citizens and judicial authorities may contribute to perceptions of injustice and distrust in the law. Likewise, situations in which persons found guilty by a court are not subjected to fair and proportionate punishment may further undermine public confidence in the justice system. These circumstances demonstrate that combating fraud remains an issue of significant relevance today.

It is well known that in recent years, the number and prevalence of cyber fraud offenses committed through the use of information technologies have been steadily increasing.

In this regard, the information and telecommunications capabilities of the population of our country have developed significantly in recent years. The development of modern society and the accelerating pace of life require the active introduction of the latest achievements in information technology into everyday life, as well as the globalization of information processes. Such technologies and opportunities are being used in virtually all-important areas of life, including education at all levels and in various types of educational institutions, from general secondary schools to higher education institutions.

They are used for presenting educational materials, participating remotely in videoconferences, providing distance education, and other purposes. Information technologies are also widely applied in healthcare, including medical consultations, remote surgical procedures, and the testing of medical equipment. In the field of commerce, they are used for concluding transactions and sending documents by electronic mail, making payments, and performing other activities.

The decline in the prices of mobile phones and other mobile devices has made it possible for a large proportion of citizens to own such devices. Consequently, almost every person in different age groups possesses at least one mobile phone.

As a result of these technological developments, members of society have become active users of social networks, mobile applications, electronic mail, and other services provided through the Internet, both for personal purposes, such as paying for utilities and educational services, and for professional and business purposes, such as making payments for goods under contracts and paying employees' wages.

The introduction of salary payment projects and the transition to electronic payment systems for personal use have become one of the social factors contributing to the increase in the number of fraudulent activities. At the same time, electronic payment systems are managed through personal accounts or by using the Internet. In this context, website developers and owners of online stores may request information concerning payment card numbers and expiration dates in order to carry out

transactions through bank accounts.

Through these systems, various monetary transactions can be conducted within the limits established by banks. In many cases, reversing such transactions, even by contacting the bank, is extremely difficult. All of these developments have contributed to a situation in which a significant proportion of the population, regardless of age, no longer carries cash on a regular basis. Consequently, in recent years, incidents of robbery and other forms of violent property crime have decreased in some contexts, while certain forms of property crime have shifted toward the so-called "cashless environment." As a result, virtually all adult members of society who have access to and the ability to use banking products and mobile devices may potentially become victims of fraud.

According to official data, the damage caused by such fraudulent activities amounts to billions of Uzbek soums annually. Furthermore, law enforcement practice demonstrates that many victims do not immediately report crimes committed against them to the relevant authorities. One of the reasons for this is the false information and misconceptions deliberately instilled in victims by offenders.

The concept of "cybercrime" encompasses a wide range of unlawful acts committed through information and communication technologies, including cyberattacks, the creation and dissemination of viruses and other malicious software, the production and distribution of unlawful information, mass distribution of electronic messages (spam), hacking attacks, unauthorized access to websites, fraud, violations of data integrity and copyright, and the theft of credit card numbers and banking information through methods such as phishing and pharming, as well as other forms of unlawful conduct.

Cyber fraud may be defined as the unlawful acquisition of individuals' personal data and financial resources through the use of the Internet and digital technologies.

The commission of fraud through the use of information systems, including information technologies, as provided for in Article 168, Part 3, Clause "c" of the Criminal Code of the Republic of Uzbekistan, refers to the misappropriation of property through deception by manipulating computer equipment, communication devices, tablets, or other similar technical devices, including property held by financial institutions, banks, funds, and other organizations.

Such fraud may be committed by altering information processed within a computer system, stored on relevant information media, or transmitted through data communication networks, as well as by entering false information into a computer system.

When distinguishing fraud committed through the use of an information system, including information technologies, from theft committed through unlawful (unauthorized) access to or use of an information system, it should be taken into account that in the case of fraud, In cases where, as a result of deception or abuse of trust, the victim voluntarily transfers his or her property or the right to such property to the possession of the offender through the use of information technologies, the victim must be aware that the property is leaving his or her possession. If a person prepares a forged document using computer technology and subsequently uses it to obtain property, the act cannot be classified under Article 168, Part 3, Clause "g" of the Criminal Code of the Republic of Uzbekistan.

The criminological characteristics of crimes committed in cyberspace in the Republic of Uzbekistan, particularly cyber fraud involving property, have been systematically studied by S.S. Gulyamov. According to the scholar, the concept of cyberspace and the dynamics of offenses committed within it differ from traditional crimes due to their transboundary and virtual nature.

At the same time, issues concerning the determinants of cybercrime and the deformation of the criminal personality have been reflected in the research of A.O. Khalmuratov . In analyzing the genesis of cybercrime, he emphasizes the significant role of victimological factors and technological vulnerabilities in the criminological characteristics of crimes committed through information technologies.

In addition, I.Abdiyakimov has conducted research on the methods of committing property crimes in cyberspace and on improving the organizational and legal mechanisms for their prevention . The author substantiates the view that the level of protection of personal data in the digital environment constitutes one of the major obstacles to the effective prevention of cyber fraud.

Furthermore, the study of the criminal-law and criminological aspects of cybercrime is one of the most relevant areas of contemporary legal scholarship. The studies of a number of leading foreign scholars have

provided an important theoretical and methodological foundation for the development of the conceptual framework of this problem.

In particular, in their early studies, Yu.M. Baturin and A.M.Jodzishvili scientifically substantiated the degree of social danger posed by crimes involving computer data . Scholars such as I.R. Begishev, M.A. Efremova , and U.V. Zinina have examined the objective and subjective elements of crimes against information security from the perspective of contemporary criminal law. T.M. Lopatina, in turn, has studied the criminal-law and criminological foundations of combating computer crime as an integrated system.

Furthermore, approaches to the criminological characterization of cybercrime and its genesis are of considerable theoretical significance. In this regard, the works of V.B. Vekhov on the methodology for investigating crimes committed through the use of computer technologies have served as an important foundation.

While the organizational and legal aspects of preventing crime in global networks have been addressed in the studies of A.L.Osipenko , R.I. Dremlyuga and T.L.Tropina have examined the criminological determinants and development trends of Internet crime. In addition, I.G. Chekunov has proposed a concept for improving criminological measures aimed at combating crimes involving computer data.

Furthermore, the works of A.G. Volevodz are particularly noteworthy in the areas of comparative legal research and international cooperation. He has developed legal mechanisms for providing international legal assistance in combating cybercrime and addressing transnational cybercrime.

Research in this area has been complemented by the studies of scholars such as V.V. Khilyuta and V.A. Golubev , who have focused on analyzing international experience in ensuring information security. K.N.Evdokimov , in turn, has developed a comprehensive system of theoretical, legislative, and practical provisions, proposals, and recommendations aimed at combating modern computer crime under conditions in which it is increasingly evolving into techno-tronic crime.

Summarizing the scholarly contributions discussed above, it can be stated that contemporary legal scholarship has developed a comprehensive and

systematic approach to cybercrime. The evolution of research demonstrates that offenses committed in cyberspace are not merely technical in nature but also have profound social, psychological, and criminological roots. In this context, in order to understand the criminological nature of property crimes committed in cyberspace, particularly cyber theft and cyber fraud, it is first necessary to systematize the existing scholarly schools and conceptual approaches in this field.

Criminological studies indicate that three principal determinants can be identified in the characterization of property crimes committed in cyberspace. These include:

Technological determinants. As emphasized by I. Abdihakimov and K.N. Evdokimov, vulnerabilities within information systems and inadequate protection of personal data may serve as a “digital key” for offenders. Today, while theft is commonly committed through unauthorized access to computer systems (hacking), fraud is increasingly associated with the use of social engineering techniques.

Victimological determinants. As demonstrated in the works of R.I. Dremlyuga and T.L. Tropina, low levels of users’ digital literacy and their susceptibility to “virtual trust” constitute major drivers of cyber fraud. The fact that a victim may facilitate the commission of a crime through his or her own actions, for example, by following a phishing link or disclosing a verification code, represents one of the most significant manifestations of victimological vulnerability in cyberspace.

Transnational nature (international scope). Drawing on the concept developed by A.G. Volevodz, it may be argued that property-related cybercrimes are often planned in one country, carried out through a server located in a second country, and directed at appropriating the funds of a victim who is a citizen of a third country.

Based on the foregoing analysis, it should be emphasized that identifying the distinguishing characteristics between cyber theft and cyber fraud is of considerable scientific importance for the criminological characterization of property crimes committed in cyberspace. In particular, cyber theft generally involves the secret appropriation of property through unauthorized access to a computer system (hacking), whereas cyber fraud is increasingly associated with various forms of social engineering.

At the same time, an analysis of the shortcomings encountered in practice in combating fraudulent offenses

in the virtual environment indicates that the following factors should be taken into account in order to improve the effectiveness of measures aimed at combating this type of crime:

Harmonization of the regulatory framework. Regulatory documents governing strategies for combating fraud in cyberspace should be systematized into a coherent regulatory framework and further developed and adapted to the practical needs of personnel responsible for combating such offenses.

Greater involvement of the public. Effective mechanisms should be established for involving the public in combating fraud in cyberspace. This requires strengthening public awareness through mass media and other communication channels regarding the material, moral, and, in certain cases, physical harm that cyber fraud may cause to individuals and society as a whole. Public awareness and educational campaigns should therefore be expanded and intensified.

Expansion and improvement of prevention and enforcement measures. Taking into account the covert and concealed nature of fraudulent offenses committed in cyberspace, it is necessary to expand the scope of measures aimed at combating such crimes and improve their effectiveness and quality.

Strengthening interagency cooperation. Reliable, effective, and coordinated cooperation should be established among all relevant services of the Ministry of Internal Affairs of the Republic of Uzbekistan, the State Security Service, customs authorities, the Department for Combating Economic Crimes under the General Prosecutor’s Office, and other law enforcement agencies, as well as banks, financial institutions, and organizations involved in electronic payment and monetary transactions. Such cooperation should ensure the timely exchange of information, coordinated responses to cyber fraud, and effective prevention and investigation of property crimes committed in cyberspace.

The implementation of the following proposals in practice may contribute significantly to improving the effectiveness of preventing fraudulent offenses in cyberspace and establishing effective mechanisms for their early prevention:

Integration of information systems. Existing software systems used by law enforcement agencies and other relevant institutions should be integrated into a unified platform to ensure that all relevant stakeholders have

appropriate access to and can effectively use the necessary information. In addition, district and city-level internal affairs bodies should be provided with modern, high-performance servers capable of ensuring the reliable and efficient operation of newly developed software systems.

Strengthening specialized personnel capacity. In view of the increasing number of complaints concerning cyber fraud and cases involving the unlawful appropriation of funds from citizens' bank cards through the use of information technologies, staffing arrangements should be reviewed and specialized personnel with appropriate technical and investigative expertise should be recruited and trained.

Increasing public awareness and digital financial literacy. Bank cardholders should be advised to exercise particular caution when purchasing goods and services through websites and online stores. Users should carefully review the terms and conditions of purchases and the public offer of the relevant website, handle payment cards responsibly, and take appropriate measures to prevent unauthorized persons from obtaining or using their card information.

Ensuring effective enforcement of liability for cyber fraud. For the purposes of preventing fraudulent offenses in cyberspace, consideration should be given to establishing mechanisms under which persons convicted of such offenses are required to serve the prescribed sentence in full until the damage caused by the offense has been compensated, where such a measure is consistent with applicable criminal-law principles and legislation.

Strengthening cybersecurity and digital culture. Ensuring reliable cybersecurity within the information systems of enterprises, educational institutions, and households, together with improving Internet users' awareness and developing responsible digital-use practices, is of particular importance for the effective prevention of fraudulent offenses committed in cyberspace.

The practical implementation of these measures would contribute to strengthening institutional capacity, increasing public awareness, improving cybersecurity, and enhancing the effectiveness of early prevention and detection of cyber fraud.

References

1. Чориев Ш. Мамлакатимизда киберхавфсизлик ва кибержиноятларга қарши курашишда амалга оширилаётган ислохотлар //Евразийский журнал права, финансов и прикладных наук. – 2022. – Т. 2. – №. 12 Special Issue. – С. 147-153. Гулямов С.С.Киберхуқук (Cyber Law). Дарслик. – Тошкент: ТДЮУ нашриёти, 2023. –Б. 112-115.
2. Khalmuratov A.Genesis of Cybercrime and its Concept Peculiarities // International Journal of Law and Criminology. –2024. –Vol. 4. –No. 01. –P. 34-39
3. Абдихакимов И. Рақамлимаконда шахсий маълумотлар дахлсизлигини таъминлашнинг ҳуқуқий муаммолари// Юридикфанлаҳборотномаси. –2023. –№4. –Б. 45-50.
4. Батурин Ю.М., Жодзишский А.М.Компьютерная преступность и компьютерная безопасность. –М.: Юрид. лит., 1991. –160 с.
5. Бегишев И.Р. Уголовная ответственность за изготовление, хранение, перевозку или сбыт специальных технических средств, предназначенных для негласного получения информации. –Казань, 2010. –С. 45–52.
6. Ефремова М.А.Уголовно-правовая охрана информационной безопасности. Монография. – М.: Юрлитинформ, 2017. –С. 88–104.
7. Зинина У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве. Дисс. ... канд. юрид. наук. –М., 2007. –С. 112–120.
8. Лопатина Т.М.Криминологические и уголовно-правовые основы противодействия компьютерной преступности. Дисс. ... докт. юрид. наук. –М., 2006. –С. 145–160.
9. Вехов В.Б. Особенности расследования преступлений, совершаемых с использованием средств электронно-вычислительной техники. – М.: ЦИиНМО КП МВД России, 2000. –С. 12–18.
10. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт. –М.: Юрлитинформ, 2004. –С. 210–225.
11. Дремлюга Р.И. Интернет-преступность: монография. –Владивосток: Изд-во Дальневост. ун-та, 2008. –С. 134–150.
12. Тропина Т.Л. Киберпреступность: понятие, состояние, тенденции развития. Дисс. ... канд. юрид. наук. –Владивосток, 2005. –С. 67–82.
13. Чекунов И.Г. Криминологическое

- противодействие преступлениям в сфере компьютерной информации. Дисс. ... канд. юрид. наук. –М., 2010. –С. 95–110.
14. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. –М.: Юрлитинформ, 2002. –С. 340–355.
15. Хиллута В.В. Преступления против информационной безопасности: проблемы квалификации. –Гродно: ГрГУ, 2005. –С. 44–58
16. Голубев В.А. Расследование компьютерных преступлений. –Запорожье: ПГУ, 2002. –С. 118–130
17. Евдокимов К.Н. «Противодействие компьютерной преступности: теория, законодательство, практика» М.: 2021. –С. 15.
18. И. Абдирахимов. Рақамли маконда шахсий маълумотлар дахлсизлигини таъминлашнинг ҳуқуқий муаммолари// Юридикфанлараборотномаси. –2023. –№4. –Б. 45-50.
19. Евдокимов К.Н. Противодействие компьютерной преступности: теория, законодательство, практика: Монография. –Иркутск: ИЮИ (ф) УП РФ, 2021. –180 с.
20. Дремлюга Р.И. Интернет-преступность: монография. –Владивосток: Изд-во Дальневост. ун-та, 2008. –240 с.
21. Тропина Т.Л. Киберпреступность: понятие, состояние, тенденции развития: Дисс. ... канд. юрид. наук. –Владивосток, 2005. –234 с.
22. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. –М.: Юрлитинформ, 2002. –496 с.