The OSCAR PUBLISHING Services
International Journal of Law And Criminology

VOLUME Vol.06 Issue03 2026
PAGE NO. 40-42
DOI 10.37547/ijlc/Volume06Issue03-07

Theoretical and Legal Challenges in The Qualification of Crimes Committed in Cyberspace

Ogamurodov Bakhriddin Bobirovich

Master's student, Tashkent State University of Law the specialty "Theory and Practice of the Application of Criminal Legislation", Uzbekistan

Received: 12 February 2026; **Accepted:** 08 March 2026; **Published:** 31 March 2026

Abstract: This article provides a comprehensive analysis of the theoretical and legal challenges that arise in the process of qualifying crimes committed in cyberspace. Particular attention is devoted to issues related to the determination of the constituent elements of a crime, as well as to the identification of the locus delicti.

Keywords: Cyberspace, cybercrime, crime qualification, elements of crime, causal nexus, information technologies, anonymity.

Introduction: Since the advent of the Internet, humanity has witnessed remarkable progress driven by the rapid development of information and communication technologies. In contemporary society, the global Internet network has become deeply embedded in virtually all spheres of human activity. Individuals routinely rely on the Internet in various domains, including education, professional activities, and travel; in essence, it permeates every aspect of daily life. While the proper utilization of the Internet offers extensive opportunities and benefits, technological advancement has simultaneously generated a range of adverse consequences. Among the most significant and potentially harmful of these consequences is the proliferation of cybercrime.

At present, cybercrime poses a substantial threat not only to individuals and organizations but also to the security and stability of entire states. In particular, such criminal activities may result in the unlawful acquisition of personal data, the disclosure of corporate trade secrets, and damage to state информационных resources. These developments, in turn, can lead to considerable economic losses, the disruption of information security systems, and even the emergence of tangible threats to national security. Although legal frameworks have established liability for such acts, one of the most pressing issues in this domain remains the existence of theoretical and legal challenges in the accurate determination of criminal liability. Specifically, the qualification of acts committed in cyberspace continues to present significant practical difficulties. Consequently, there is a growing necessity to develop scientifically substantiated approaches and to reassess existing theoretical paradigms in order to adapt them to the realities of modern digital relations.

One of the most crucial and, at the same time, complex issues in the qualification of crimes committed in cyberspace is the accurate identification of the constituent elements of a crime. Within the framework of criminal law, the elements of a crime traditionally comprise the object, the objective side, the subject, and the subjective side, and their determination is generally based on relatively stable and well-established criteria. However, contemporary legal practice reveals a number of theoretical and legal challenges in identifying these elements in the context of cybercrime.

First and foremost, the determination of the object of the crime requires particular scrutiny. In conventional criminal law, the object is typically understood as specific social relations, such as property, personal rights, or public safety. In contrast, in the context of cybercrime, this concept acquires a broader and more complex character. This is attributable to the fact that the harm inflicted by such crimes is often directed not toward tangible objects but toward information

resources, databases, or the proper functioning of information systems. Accordingly, the question of which social relation should be recognized as the primary object remains subject to ongoing theoretical debate. From our perspective, it is appropriate to prioritize social relations associated with information security when determining the object of cybercrime.

Another essential element is the objective side of the crime. Traditionally, the objective side encompasses the external manifestation of a criminal act, including the socially dangerous conduct (whether by action or omission), its consequences, and the causal nexus between them. However, in cybercrime, actions are frequently executed indirectly through technical means rather than through direct physical conduct. For instance, acts such as the dissemination of malicious software, unauthorized access to information systems, or the manipulation of data differ substantially from traditional forms of criminal behavior. This divergence complicates their precise legal characterization.

In particular, establishing the causal nexus between the socially dangerous act and its resulting consequences constitutes one of the most challenging aspects in practice. Demonstrating the connection between an action performed in cyberspace and the ensuing harm often necessitates specialized technical expertise. For example, determining whether a system malfunction is attributable to a specific unlawful act or to unrelated technical failures represents a complex and technically demanding process. In this regard, expert technical assessments assume a decisive role in the qualification of cybercrime.

The issue of the subject of the crime also presents distinctive challenges in the context of cybercrime. Under criminal law, the subject is defined as a sane natural person who has reached the age of criminal responsibility. However, due to the inherently high level of anonymity in cyberspace, identifying the perpetrator becomes significantly more difficult compared to traditional crimes. The use of various technologies, including VPN services, anonymous accounts, and other digital tools, considerably enhances the ability of offenders to conceal their identity. As a result, the processes of identifying the subject of the crime and attributing legal responsibility are substantially complicated.

The subjective side, namely the form of guilt, likewise necessitates a differentiated approach in cybercrime cases. Although the majority of cybercrimes are committed intentionally, elements of negligence may occasionally be present. Nevertheless, establishing the precise intent of an individual within the digital environment is not always straightforward, given that actions are often carried out indirectly посредством technical means. This circumstance gives rise to additional complexities in determining the form of guilt.

Another particularly complex issue in the qualification of crimes committed in cyberspace is the determination of the place where the crime was committed. In traditional criminal law, this issue is generally resolved by reference to the location where the socially dangerous act occurred. In the context of cybercrime, however, the situation is considerably more intricate, as such offenses frequently involve multiple jurisdictions. Specifically, the perpetrator may be located in one country, the affected information system in another, and the data stored in yet another location.

For example, an individual located in State A may, without leaving that territory, unlawfully access an information system in State B and cause damage to it. In such circumstances, the question arises as to where the crime should be deemed to have been committed—whether in State A, where the act was initiated, or in State B, where the harmful consequences materialized. In practice, the absence of a unified approach to this issue often results in jurisdictional conflicts.

In an effort to address these challenges, several international legal instruments have been developed. Among them, the Budapest Convention on Cybercrime of 2001 occupies a prominent position. Although Article 22 of this Convention addresses issues of jurisdiction, it does not fully resolve the problem of determining the locus delicti in cybercrime cases. Furthermore, the borderless nature of the Internet, coupled with the widespread use of modern technologies such as cloud computing, further complicates the determination of the territorial nexus of criminal activity.

The foregoing analysis demonstrates that the determination of both the constituent elements of cybercrime and the place of its commission differs substantially from traditional approaches in criminal law. Accordingly, there is an increasing need to adapt existing theoretical frameworks to contemporary technological realities and to develop new, more flexible, and comprehensive criteria for identifying the elements of a crime and its territorial scope.

At present, these unresolved issues constitute one of the principal obstacles to the proper qualification of cybercrime. Therefore, addressing these challenges requires the development of scientifically grounded approaches, the refinement of national legislation, and an in-depth examination of international practices.

Only through such measures can an effective legal assessment and fair qualification of crimes committed in cyberspace be ensured.

REFERENCES

1. Budapest Convention on Cybercrime // 2001;
2. Criminal Code of the Republic of Uzbekistan // 1994;
3. Ochilov X. Criminal Law (General Part) // Tashkent, 2022;
4. Rustambayev M. Criminal Law // Tashkent, 2008;
5. Salaev N., Roziev R. National and International Standards in Combating Cybercrime // Monograph, Tashkent, 2018;
6. Ovliyakulov H. Types of Cybercrime and Issues of Its Prevention // Innovation Science and Research, 02.06.2023.