

<https://doi.org/10.5281/zenodo.16861339>

S. Bahromov

Officer of the Fergana Regional Department of Internal Affairs

Abstract: *The article analyzes the term cybercrime and its essence. Opinions are given on the types and statistics of cybercrimes. Considerations are presented regarding two of the most prominent social phenomena in recent years — the globalization of crime and the emergence of the global information mega-environment.*

Keywords: *Internet, cybercrime, cyberspace, computer crime, concept, essence, Council of Europe Convention on Cybercrime.*

At present, scholars rightly believe that in the 21st century, studying the criminal situation, identifying its characteristics and trends, cannot be imagined without taking into account the most important scientific and technical phenomenon of our time — the widespread use of information technology.

In recent years, despite their different forms, two prominent social phenomena — the globalization of crime and the emergence of the global information mega-environment — have shown a tendency toward strengthening their interconnection.

This interrelationship is far removed from the purely electronic criminal phenomenon referred to as “computer crime” or “cybercrime.” The globalization of information processes and the emergence of a global information space lead to the appearance of new criminal offenses (against computers and computer networks) that have not yet been legally regulated. New methods of committing crimes appear — for example, fraud (theft) by altering or blocking computer data. Other consequences of the widespread use of computer technologies include the almost unhindered formation and dissemination of criminal ideology, and the use of the information space for criminal purposes — communication, experience sharing, and coordination of actions.

The issue of the relationship between crime and information technology encompasses several aspects:

- The problem of identifying the growth and globalization of crime through the global information environment and electronic mass media (information technology acting as a method or means of committing a crime, as well as an object of attack);
- The problem of legal regulation of processes related to the criminal use of computer technology;
- The potential of global information networks for prevention and the possibility for law enforcement agencies to use information technologies.

The first aspect of the problem — the criminal use of scientific and technological achievements — concerns identifying the growth and globalization of the information mega-environment, which is one of the most important directions of integration processes. Today, the global Internet network, which has opened wide opportunities for obtaining and exchanging information, is developing rapidly.

Of course, the development of global communication and information systems is inevitable and has many advantages. At the same time, as in other spheres of globalization, new modern means of information exchange and technological achievements are increasingly used for criminal purposes, which in turn become factors of crime globalization.

According to international classifications, computer crimes that affect the processes of crime reproduction include:

- Use of electronic bulletin boards (BBS) for storing, exchanging, and distributing materials related to criminal activity;
- Theft of data constituting trade secrets;
- Obtaining or transmitting information representing trade secrets by illegal means with the intent to cause economic damage or obtain illegal economic benefits without legal justification;
- Use of computer systems or networks to store, exchange, distribute, or transfer confidential information.

In general, the distinctive features of cybercrimes include:

- Such crimes have no territorial boundaries and can be expected from anywhere in the world at any time;
- The constant creation of new, more dangerous viruses and other malicious programs;
- The lack of qualified specialists with deep knowledge in the field in agencies combating cybercrime, leading to late detection of crimes;
- The loss of ownership rights not to physical property, but to information as a result of cybercrime;
- Errors in data processing may go unnoticed and uncorrected in time, making it impossible to prevent future mistakes;
- Computer crimes are often not reported in time (to hide network vulnerabilities, preserve institutional reputation, or for other purposes);
- The specific difficulty of investigating and detecting cybercrime, its potentially huge damage, and the absence of a unified legal basis for combating and preventing it.

It is clear that cybercrime should be distinguished both as a legal category and as a social phenomenon.

The Internet is increasingly used to commit criminal activities. For example, terrorists may use it to discredit governments and states, host terrorism-related websites, insert false information, or damage and destroy key systems by regularly shutting them down —

all due to the Internet's openness. The Internet is also used to arrange prohibited sexual relations, promote prostitution markets, and distribute obscene materials and pornography. Cyberspace allows the use of pseudonyms instead of real names, making it easier to establish contacts with partners.

Specialists note that while such crimes are most typical for the online environment, criminals can use email for almost any illegal actions, including threats, blackmail, and extortion. Because reliable encryption methods are widespread, criminals may use this technology to avoid detection when planning and carrying out any illegal activity.

The concept of global cyberspace is still unusual for law enforcement agencies, but criminal activities involving computer communications pose a great social danger. Computer crimes are dangerous not only by themselves but also because they contribute to committing ordinary crimes, expanding the scope of criminal activity.

The growing influence of mass media is closely linked to the criminalization of public consciousness. Promoting cruelty, violence, and deviant sexual behavior on the Internet requires awareness of its consequences.

Many online resources are devoted to pornography, matchmaking, and searching for sexual partners. A significant part of Internet resources is dedicated to instructions for producing narcotics and explosives at home. It is likely that some terrorists have completed online training courses similar to "young fighters' courses" on the Internet.

On the other hand, under the influence of uncontrolled use of Internet resources — considering the duration, frequency, and intensity of consuming certain information — a significant deformation of a person's moral and psychological characteristics can occur.

The most distinct and "traditional" use of information technologies by law enforcement and special services (in particular, Interpol and other international police organizations) is the creation of various types of electronic files, databases, automated data banks, and information retrieval systems at the regional, national, and international levels. This approach has been implemented since the early days of computing technology. It is sufficiently developed and has a certain positive effect, but it does not exhaust the possibilities of modern information technologies. New information technologies make it possible to track criminal groups' activities very quickly and fundamentally.

The history of cybercrime is closely linked with the history of legislation against high-tech offenses. Below we analyze this relationship. Cybercrime continues to evolve, giving rise to new forms of criminal offenses. Since the problem of cybercrime has not existed for long, the international community is still searching for effective criminal law measures and other methods to combat it. The goal is to develop a unified policy on this issue.

The development of cyberspace and the global communication technologies used within it is taking place at a very rapid pace. Therefore, factors of transboundary cyberspace that make it possible to commit illegal acts from the territory of one state under the legal norms of another state must be considered from the perspective of national legislation. An important feature of cyberspace is that it is very difficult to

determine both the exact location of criminals and the exact time certain illegal actions were committed.

A complete description of this phenomenon is complicated by two factors. First, there is currently no universally accepted definition of cybercrime. Second, due to differences in legal systems in different states and the novelty of the issue of offenses, the term “cybercrime” is not applied as a legal term in all countries of the world.

The term “cybercrime” is currently often used together with the term “computer crime,” and often as a synonym.

Indeed, these terms are very close, but they are not exact synonyms. In our opinion, the concept of “cybercrime” (in English — cybercrime) is broader than “computer crime” and more accurately reflects the nature of the phenomenon as a crime in the information space. The Oxford Dictionary defines the prefix “cyber-” as relating to information technology, the Internet, or virtual reality. The Cambridge Dictionary gives a similar definition: “Cyber-” is a prefix meaning “using computers or relating to computers, especially the Internet.” Thus, “cybercrime” refers to crimes involving both the use of computers and the use of information technologies and global networks. Meanwhile, the term “computer crime” refers only to crimes against computers or computer data. The integration of mobile communication devices with the Internet is called the “mobile revolution” by specialists. Telecommunications infrastructures have adapted to maximize the movement of large volumes of data in the most convenient form for the consumer.

For the above reasons, the term “computer crime” no longer covers all crimes in this area. Researchers have proposed various solutions to this problem. For example, there is a viewpoint that “computer crimes” should be classified as “direct computer crimes” and “related crimes.”

Thus, it turns out that the term “computer crime” refers to a much wider range of actions than its literal meaning suggests. In our opinion, this position is not entirely correct. The main point, however, is true — the terms “computer crime” and “computer-related crimes” carry less semantic weight and do not precisely define all the actions they describe. Therefore, such offenses should be divided into “direct computer crimes” and “related crimes.” From our point of view, it is necessary to give a broader definition of this type of crime, one that covers both computer crimes and crimes related to them. In this context, the definition of “cybercrime” is more appropriate.

According to D.N. Karpova, cybercrime is a socially dangerous act committed using any technical means with access to the Internet, aimed at causing economic, political, moral, ideological, cultural, or other types of harm to an individual, organization, or state. Karpova also considers ideological harm to an individual as cybercrime.

Thus, the development of a conceptual framework is the first step in combating cybercrime in criminal law. The definition of cybercrime should be approached with caution. Due to the specific nature of such crimes, the legislation to combat them should be adopted in accordance with special international documents (such as the Council of

Europe Convention on Cybercrime), because effective combat against cybercrime is currently impossible within the borders of a single country without international cooperation.

REFERENCES:

1. Drëmin V. N. Globalization of information systems as a factor in the globalization of crime // Information Technology and Security. – Kyiv, 2002. – p. 57.
2. Roziyev R. N., Salaev N. S. National and international standards on combating cybercrime. Monograph. – Tashkent: Tashkent State University of Law, 2018, p. 6.
3. www.statista.com
4. Oxford English Dictionary [Electronic resource]. Available at: <http://www.askoxford.com/> [Accessed: 29.12.2023].
5. Cambridge Advanced Learner's Dictionary [Electronic resource]. Available at: <http://dictionary.cambridge.org> [Accessed: 29.12.2023].
6. Lyapunov Yu., Maksimov V. Liability for computer crimes and Legality. – 1997. – No. 1. – pp. 8–9; Sergo A. Internet and Law. Moscow, 2003. – pp. 217–218.
7. Karpov V. S. Criminal liability for crimes in the field of computer information. Abstract of the dissertation for the degree of Candidate of Legal Sciences. – Krasnoyarsk, 2002. – p. 16.
8. Karpova D. N. Cybercrime: a global problem and its solution. Vlast, 2014, p. 47.