Modern American Journal of Social Sciences and Humanities
ISSN (E): 3067-8153
Volume 2, Issue 5, May, 2026
Website: usajournals.org

SOCIO-PHILOSOPHICAL FOUNDATIONS OF COMBATING CYBERCRIME IN THE CONTEXT OF DIGITAL SOCIETY

Bahromov Saidolimkhon Saidalikhon corner
Independent Applicant, Fergana State University

Abstract
This article examines the socio-philosophical foundations of combating cybercrime in the context of digital society. The rapid development of digital technologies, the expansion of the information space, and the digitalization of all spheres of social life have led to the emergence of new forms and increasing scale of cybercrime. Therefore, addressing cybercrime requires not only legal and technological solutions but also comprehensive socio-philosophical analysis. The paper explores the social factors influencing cybersecurity, including information culture, digital literacy, moral and ethical values, individual digital responsibility, and the establishment of trust within the digital environment. Particular attention is paid to the socio-philosophical justification of the roles of the state, civil society institutions, and the education system in preventing cybercrime. The study concludes that effective cybercrime prevention is achievable only through an integrated approach combining legal, technological, social, and moral mechanisms.
Keywords: Digital society, cybercrime, cybersecurity, social philosophy, digital culture, digital literacy, information security, moral and ethical values, digital responsibility.

INTRODUCTION (Video/Introduction).

In the 21st century, digital technologies have become an integral part of human life, bringing about fundamental changes in the fields of economy, politics, education, medicine, public administration and social communication. The widespread use of artificial intelligence, big data, cloud technologies, internet networks and digital platforms is shaping a new stage of social development - the

Modern American Journal of Social Sciences and Humanities
ISSN (E): 3067-8153
Volume 2, Issue 5, May, 2026
Website: usajournals.org

digital society. However, along with positive opportunities, this process also creates cybercrime, illegal distribution of personal data, information manipulation, digital fraud, cyberterrorism and other risks.

Today, cybercrime has a transnational nature, and its economic, political and social consequences are becoming increasingly serious. Therefore, there is an increasing need to study this problem not only from a legal or technical point of view, but also as a socio-philosophical issue related to the system of relations between a person, society and the state. After all, ensuring cybersecurity is not limited to technical means; it is inextricably linked with the information culture of a person, digital literacy, spiritual immunity, social responsibility and the culture of using information.

Reforms aimed at developing the digital economy, digitizing public services, and improving the e-government system in Uzbekistan are making the scientific study of the socio-philosophical aspects of ensuring cybersecurity even more relevant. In particular, issues such as individual rights in the digital space, freedom of information, digital ethics, and raising the legal awareness and cyberculture of citizens are among the priority scientific areas today.

At the stage of development of the new Uzbekistan, priority tasks have been set, aimed at ensuring the rights and interests of citizens, forming a stable civil society, and ensuring that national criminology takes a worthy place in international rankings, based on the principle of "For the sake of human dignity."[1]In this context, it is necessary to prevent criminal trends observed in the field of information technologies, ensure security in cyberspace, improve effective organizational and legal mechanisms, and create a reliable architecture for the dissemination of information.[2]The creation of is gaining scientific and practical importance today. Human development is developing in close connection with digital technologies, artificial intelligence, Internet communications and global information systems. The formation of a digital society has deeply penetrated all aspects of human life. State administration, economy, education, medicine, banking system, social communications and

[1]Development Strategy of New Uzbekistan for 2022-2026. –Tashkent: Adolat National Legal Information Center. 2022. –P.4.
[2]On measures to organize scientific and practical research in the field of criminology / Resolution of the President of the Republic of Uzbekistan dated 15.01.2024 No. pq-22.

Modern American Journal of Social Sciences and Humanities
ISSN (E): 3067-8153
Volume 2, Issue 5, May, 2026
Website: usajournals.org

cultural processes are increasingly digitized. Although this situation is creating a new civilizational stage of human development, it is also creating new dangers and threats. One of the most urgent manifestations of such global threats is cybercrime.

Cybercrime today is not only a technological or legal problem, but also a complex socio-spiritual and philosophical phenomenon. Because cybercrime directly affects the human mind, moral values, spiritual environment and social relations. Therefore, technical means or legal mechanisms alone are not enough to combat cybercrime. In this process, the development of social consciousness, spiritual immunity, information culture and digital ethics come to the fore as important determinants.

Philosophically, cybercrime is interpreted as a negative product of technogenic civilization. While technological progress has created enormous opportunities for humanity, it can also become a dangerous tool in the face of human spiritual uncontrollability and moral crisis. This brings to the agenda the issue of the balance between technology and spirituality. Martin Heidegger noted that technology can change human thinking and turn a person into a simple element of a technological system. Today, fraud, manipulation, cyberterrorism and information wars committed in virtual space are seen as the negative consequences of this technogenic thinking.

Literature analysis and methodology (Literature and methodology /Methods).

It has become necessary to conduct extensive scientific research devoted to the philosophical analysis of the essence of cybercrime, its transformation processes and its contradictory effects on the socio-cultural environment in leading scientific and research institutions and centers around the world. For example, (United Nations Office on Drugs and Crime), (Global Cybercrime Programme) under INTERPOL, European Cybercrime Centre (EC3), (Software Engineering Institute and CERT Coordination Center), (Cooperative Cyber Defence Centre of Excellence), Kaspersky Global Research and Analysis Team and IBM X-Force[3]It

[3]https://www.cybersecurityintelligence.com/europol---european-cybercrime-centre-ec3-9300.html.

Modern American Journal of Social Sciences and Humanities
ISSN (E): 3067-8153
Volume 2, Issue 5, May, 2026
Website: usajournals.org

is engaged in studying the transnational risks of cybercrime, strengthening international cooperation, and developing legal mechanisms for states. Therefore, in the conditions of an increasingly digital society, there is an increasing need for comprehensive research into the socio-philosophical mechanisms and factors of preventing cybercrime.

The rapid development of digital technologies and their deep introduction into all spheres of social life are fundamentally changing the scope and nature of threats in the cyber environment. Along with the expansion of information systems, electronic services and digital infrastructure, threats to cybercrime are becoming more complex not only in terms of quantity but also in terms of content, and their level of social danger is increasing. This situation requires the identification of the fight against cybercrime as one of the priority tasks of strategic importance in modern society.

Cybercrime threats directly affect the national security, economic stability, information sovereignty, and the rights and freedoms of citizens. In particular, the transnational nature of cyberattacks, the high level of anonymity, and the easy accessibility of the means of committing crimes reduce the effectiveness of traditional legal and organizational mechanisms in combating them. Therefore, combating cybercrime requires a comprehensive and systematic approach, not limited to punitive measures alone.

Modern scientific research and international experience show that effective combating of cybercrime should be carried out by combining legal, organizational, technical and social measures. Ensuring cybersecurity, protecting digital infrastructure, increasing the information culture of the population and strengthening international cooperation are emerging as priority areas in this area. However, the systematization of these areas on a scientifically based basis and their implementation taking into account national characteristics remains an urgent issue.

In this context, identifying priority areas for combating cybercrime threats in modern society and scientifically analyzing them is of significant theoretical and practical importance for the formation of effective state policies and legal mechanisms, as well as for creating a stable system in the field of cybersecurity.

Modern American Journal of Social Sciences and Humanities
ISSN (E): 3067-8153
Volume 2, Issue 5, May, 2026
Website: usajournals.org

In recent years, the rapid development of digital technologies has affected all aspects of society, as well as radically changed the nature of crime and the methods of its implementation. As a result of the expansion of cybercrime, new, highly complex and cross-border threats are emerging in the criminological environment, which are not typical of traditional crime. Such crimes are manifested in such forms as theft of personal data, financial fraud, distribution of malicious programs, disruption of digital infrastructure and dissemination of destructive information that affects social consciousness. The negative impact of cybercrime is not limited to technical or economic aspects. It weakens confidence in security in society, encourages new types of crime, increases the propensity for criminal activity in the minds of young people, and serves to expand the criminogenic environment. Therefore, studying the destructive impact of cybercrime on the criminological environment, analyzing its social consequences, and developing effective preventive measures are urgent tasks for modern society.

Results (Results)

The globalization of information processes and the emergence of a global information space lead to the emergence of new objects of criminal aggression (computers and computer networks) that are not yet legally regulated. New methods of committing crimes appear: for example, fraud (theft) by changing or blocking computer data. Other consequences of the widespread use of computer technologies are the almost unhindered formation and propagation of criminal ideology, the use of the information space for criminal purposes - for communication and exchange of experience, coordination of actions. The problem of the relationship between crime and information technologies is divided into several aspects, namely:

- the problem of determining the growth of crime and its globalization by the information mega-world and electronic media (information technologies act as a method or tool for committing crimes, as well as an object of aggression);
- the problem of legal regulation of processes related to the criminal use of computer technologies;

Modern American Journal of Social Sciences and Humanities
ISSN (E): 3067-8153
Volume 2, Issue 5, May, 2026
Website: usajournals.org

- the preventive capabilities of global information networks and the use of information technologies by law enforcement agencies. The first aspect of the problem, the problem of using scientific and technical achievements for criminal purposes, is one of the most important directions of integrated processes, which is the growth of the information mega-environment and the process of globalization. Today, the global Internet, which has opened up wide opportunities for obtaining and exchanging information, is developing very rapidly. Cyberterrorism (cybercrime, cyberwar) is an attack on computer and Internet systems, a threat to the individual, society and the state using modern information and communication media technologies[4]. According to data from April 2020, the number of Internet users in Uzbekistan reached 18.4 million (which corresponds to 55% of the total population), 76% of the population or 25.14 million Uzbeks own mobile phones, as well as access to international networks from Uzbekistan. The total connection speed was 104.1 Gbit/s.[5]. Currently, there are more than 66 thousand active domains in the national domain "UZ". In 2017, there were about 53 thousand active domains in Uzbekistan, and in 2018 their number reached 65 thousand.The State Statistics Committee's report on how many residents of Uzbekistan are connected to the Internetaccording to informationAs of January 1, 2020, the number of subscribers connected to the Internet amounted to 16 million 386 thousand 200, an increase of 23.0 percent or 3.1 million compared to the same period in 2019.Of these, there are 15.8 million subscribers among the population, which is 22.3 percent or 2.9 million more than last year.

It was reported that the largest number of subscribers was recorded in Tashkent city (3,550,600) and the smallest number of subscribers was recorded in Syrdarya region (441,400).[6].The presence of internet services in every user means that they can become victims of cyberterrorism. According to the UZCERT-Information Security Incident Response Service, during the monitoring of information security incidents in the information systems of state bodies in 2018 and the first quarter of 2019, 54,953,759 information security breaches were identified. Of

[4]K. Nazarov Encyclopedia of World Philosophy Volume I "National Society of Philosophers of Uzbekistan" "Manaviyat" Publishing House Tashkent - 2023. B-585.
[5]https://wearesocial.com/digital-2020.
[6]https://daryo.uz/k/2020/10/29/ozbekistonning-kancha-aholisi-internet-tarmogiga-ulaganan

Modern American Journal of Social Sciences and Humanities
ISSN (E): 3067-8153
Volume 2, Issue 5, May, 2026
Website: usajournals.org

these, 2,502,353 were of high risk.[7]. Of course, the development of global communication and information systems is inevitable and has many advantages. At the same time, as in other areas of globalization, new modern means of information exchange and technological advances are increasingly being used for criminal purposes. This leads to factors of globalization of crime. According to international classifiers, computer crimes that affect the processes of reproduction of crime include:

1. Using electronic bulletin boards (BBS) to store, exchange and distribute materials related to criminal activities;
2. Theft of information constituting a trade secret;
3. Unlawful acquisition or transfer of information constituting a trade secret with the intention of causing economic harm or obtaining illegal economic benefits, with the right or other legal justification;
4. It is the use of computer systems or networks to store, exchange, distribute, or transfer confidential information.[8]In general, the following are the characteristics of cybercrime:

- this category of crimes does not choose a location and can be expected at any time from different parts of the world;
- the regular creation of new and more dangerous viruses and other malicious programs every day;
- the lack of qualified specialists with excellent knowledge in this field in the bodies combating cybercrime, resulting in late detection of the crime;
- Cybercrime results in the loss of ownership of information, not specific property;
- errors made during information processing are not tracked and corrected in a timely manner, resulting in future errors not being prevented[9].
- computer crimes committed are not reported in a timely manner (to hide the existence of flaws in computer networks from others, to maintain the reputation of the institution, and for other purposes);

[7]https://uzcert.uz/blog/saidakbar/kiberbezopasnost-uzbekistana-v-tsifrah-itogi-2018-goda.
[8]V.H. Dryomin Globalization of the information system as a factor of globalization of prestupnosti // Information technology. - Kiev, 2002. - S. 57
[9]Ruziev R.N., Salaev N.S. National and international standards for combating cybercrime. Monograph. – Tashkent: TDUU, 2018, p. 6.

Modern American Journal of Social Sciences and Humanities
ISSN (E): 3067-8153
Volume 2, Issue 5, May, 2026
Website: usajournals.org

- the inherent difficulty of investigating and solving cybercrime, the enormous damage it causes, the lack of a single legal framework for combating criminals and its prevention, etc. It is clear that cybercrime should be distinguished both as a legal category and as a social phenomenon.

Discussion (Obsujdenie/Discussion).

The Internet is increasingly being used for criminal activities. For example, terrorists use the Internet's openness to commit crimes such as discrediting governments and states, hosting terrorist-oriented websites, inserting false information into them, or permanently disabling these systems to damage and destroy key systems. The Internet is used to establish pedophile (pedophile) and other forbidden sexual relationships, to create a prostitution market, to sell obscene materials, and to sell pornography. Cyberspace allows the use of pseudonyms instead of real names and makes it easier to establish contact with partners. Although experts believe that such crimes are most typical for the online environment, it is worth noting that e-mail can be used by criminals to plan or coordinate almost any illegal actions, including threats, blackmail, and extortion. As secure methods of encoding information become widespread, it can be expected that criminals will use such technology to avoid detection when planning and carrying out any illegal activity.

The concept of global cyberspace is still unfamiliar to law enforcement agencies, but criminal activities related to computer communications pose a significant social threat. Computer crimes are dangerous not only in themselves, but also because they contribute to the commission of ordinary crimes and expand the scope of criminal activity. The International Cyber Security Forum (Cyber Security Forum-2017), held in Moscow on February 7, 2017, identified three of the most common attacks in the world of cybercrime today. According to experts, most Internet users today become victims of cybercrime by stealing data through phishing, hacking into electronic devices through mobile applications with a hidden purpose, and viewing unprotected communication channels.

Today, services such as distributing information about the geographical location of a specific person or object, hacking into personal databases, etc. are popular in cybercrime. Hackers obtain such information from Internet and social network

Modern American Journal of Social Sciences and Humanities
ISSN (E): 3067-8153
Volume 2, Issue 5, May, 2026
Website: usajournals.org

users in exchange for accessing various electronic resources without reading their terms of use. According to statistics, in 2016, 600 million crimes were committed worldwide. Of these, 40 million are cybercrimes. This is more than the population of countries such as Belgium, Switzerland, Sweden. In 2018, 556 million people worldwide became victims of cybercrime per year, 1.5 million per day, and 18 per second[10]. The growing influence of mass media is closely related to the criminalization of public consciousness. Uzbekistan ranks 68th in the ranking of countries subject to cyberattacks, and 3rd in Asia.[11].Promoting cruelty, violence, and perverted forms of sexual behavior online requires understanding its consequences.

Conclusion (Zaklyuchenie/Conclusion).

The results of the study show that combating cybercrime in a digital society is a complex and multifaceted social process, the effectiveness of which directly depends not only on legal and technical measures, but also on socio-philosophical factors. Along with the development of information technologies, improving the digital culture, legal awareness, moral responsibility and knowledge of the individual in the field of cybersecurity is an important condition for the formation of a stable digital environment.

In preventing cybercrime, cooperation between government agencies, educational institutions, civil society institutions, the media, and the private sector is of paramount importance. In particular, the formation of digital literacy, information security culture, and cyberethics principles among young people will serve as one of the most effective preventive mechanisms for ensuring cybersecurity in the future.

Also, in the context of the development of a digital society, it is important to improve the socio-philosophical concept of combating cybercrime, develop scientific approaches aimed at ensuring a balance between human interests, information security and digital rights. This will not only strengthen the national

[10]www.statista.com.
[11] https://cybermap.kaspersky.com/ru/stats/., see also: Anorboev A.U. Cybercrime: criminal and legal and criminological aspects.: (PhD) diss.12.00.08.,-T., 2020, 260 p.

Modern American Journal of Social Sciences and Humanities
ISSN (E): 3067-8153
Volume 2, Issue 5, May, 2026
Website: usajournals.org

cybersecurity system, but also help form a stable, safe and spiritually harmonious digital society.

REFERENCES

1. Development Strategy of New Uzbekistan for 2022-2026. –Tashkent: Adolat National Legal Information Center. 2022.
2. On measures to organize scientific and practical research in the field of criminology / Resolution of the President of the Republic of Uzbekistan dated 15.01.2024 No. pq-22.
3.https://www.cybersecurityintelligence.com/europol-european-cybercrime-centre-ec3-9300.html.
4. Q. Nazarov Encyclopaedia of World Philosophy, Volume I "National Society of Philosophers of Uzbekistan", "Spirituality" Publishing House - Tashkent.: 2023.
5. https://wearesocial.com/digital-2020.
6.https://daryo.uz/k/2020/10/29/ozbekistonning-kancha-aholisi-internet-tarmogiga-connected.
7.https://uzcert.uz/blog/saidakbar/kiberbezopasnost-uzbekistana-v-tsifrakh-itogi-2018-goda.
8. V.H. Dryomin Globalization informatsionnykh system kak factor globalizatsii prestupnosti // Information technologist ta bezpeka. - Kyiv, 2002.
9. Ruziev R.N., Salaev N.S. National and international standards for combating cybercrime. Monograph. – Tashkent.: TDUU, 2018.
10. www.statista.com.
11.https://cybermap.kaspersky.com/ru/stats/., see also: Anorboev A.U. Cybercrime: criminal-legal and criminological aspects.: (PhD) diss.12.00.08.,-Tashkent.: 2020.