Journal Homepage: -www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI:10.21474/IJAR01/22568
DOI URL: http://dx.doi.org/10.21474/IJAR01/22568

RESEARCH ARTICLE

INTERNATIONAL LEGAL AND REGULATORY ASPECTS OF COMPUTER CRIMES IN THE FOOD SECURITY SYSTEM

Nikolay Trifonov

1. Chief Assistant,Trakia University of Stata Zagora, Bulgaria.

Manuscript Info

Manuscript History
Received: 06 November 2025
Final Accepted: 08 December 2025
Published: January 2026

Key words:-
computer crimes, United Nations, food security

Abstract

Modern computer crime necessitates criminal-law counteraction by states and the international community. It is essential to respond by establishing unified international legal norms regulating the elements of computer crimes and liability for their commission, as well as by incorporating them into national legislation.

Introduction:-

Modern computer crimes, in the context of transformation within the technotronic environment, have a cross-border and transnational character. However, in the existing cyberspace, they have no state or geographical boundaries. Computer criminals, forming a technical “underground” of the global community, are not divided by nationality. They unite in international organized criminal groups.Therefore, these characteristics of contemporary computer crime necessitate criminal-law countermeasures by states and the international community through the establishment of unified international legal norms regulating computer crimes and liability for their commission, followed by their implementation in national criminal legislation.

Methods:-

The empirical research method was used to collect and analyze data from real cases and events. A historical-logical approach was applied to reveal the objectives and tasks of the study. The framework of the research and interpretation of results relied on theoretical knowledge. The historical method was also used to analyze past events based on primary sources and other evidence, along with the general scientific method of synthesis.

Results:-

In academic circles, it is considered that the first international study of the problem of computer crime and the development by the global community of criminal-law measures to combat it—including computer crimes in the field of food security—was undertaken by the Organisation for Economic Co-operation and Development (hereinafter OECD) during the period from 1983 to 1985. This is reflected in the report Computer-Related Crime: Analysis of Legal Policy. In this report, in addition to recommendations for improving the national criminal legislation of OECD member states, a minimum list of computer-related acts subject to further criminalization by legislators was formulated (for example, intentional hacking, alteration, deletion, concealment of computer data and/or computer programs, intent to commit forgery, illegal movement of funds or other tangible assets, obstruction of the functioning of computer and/or telecommunications systems, etc.) (Kopcheva, 2006).Subsequently, on 26 November 1992, the OECD Council adopted a recommendation on guidelines for the security of information

Corresponding Author:-Nikolay Trifonov
Address:-Chief Assistant,Trakia University, StaraZago.

systems, including legal principles containing mandatory rules of criminal law providing for liability for violations of information system security.

A significant step toward the development of an international criminal-law mechanism to counter computer crime was also taken by the Council of Europe, which on 13 September 1989, at a meeting of the Committee of Ministers, adopted Recommendation No. 2 (89) 9. This recommendation includes two lists of computer crimes recommended for criminalization in the national legislation of Council of Europe member states. The first list contains a "minimum" set of offenses that are mandatory for inclusion in criminal law (e.g., computer fraud; computer forgery; damage to computer data and computer programs; computer sabotage; unauthorized access to computer networks; unauthorized interception of data; unauthorized copying of protected computer programs). The second list includes an "additional" (optional) set of computer crime offenses recommended for criminalization in the legislation of member states.In 1994, the UN Manual on the Prevention and Control of Computer-Related Crime (UN, 1994) was published, providing an overview of crimes regulated by the criminal legislation of foreign states in the field of data and information protection, including in cyberspace.

An important contribution to the development of the international criminal-law framework for combating computer crime and to law enforcement practice was made by the introduction in 1991, within the activities of the International Criminal Police Organization (hereinafter Interpol), of a computer crime codifier containing a classification of criminal acts committed using computers. This codifier has been integrated into Interpol's automated information retrieval system and is currently used in more than 100 countries. Its advantage lies in the detailed systematization of computer crimes according to the method of their commission, which provides a fairly accurate representation. For objective reasons, however, this information is incomplete, as it does not include crimes committed using modern information and communication technologies. This finding is reflected in Recommendation No. 0 (89) 9 of the Committee of Ministers of the Council of Europe of 13 September 1989.

It should be noted that the most important legal instrument defining the international criminal-law foundations for combating computer crime is the Council of Europe Convention on Computer Crime (hereinafter the Convention on Cybercrime), adopted on 23 November 2001 in Budapest. In the Convention on Cybercrime, existing computer crimes are divided into five groups (types): crimes against the confidentiality, integrity, and availability of computer data and systems (e.g., illegal access, illegal interception, data interference, system interference, misuse of devices); computer-related offenses (computer-related forgery, computer-related fraud); content-related offenses (offenses related to child pornography); offenses related to infringements of copyright and related rights; and offenses related to acts of racism and xenophobia committed through computer systems (Convention, 2005).

The Convention on Cybercrime is, in fact, the first international instrument aimed at forming a common criminal-law policy for protecting society against computer crime. It provides for the application, within the legislation of Council of Europe member states and states that have ratified the Convention, of criminal-law norms containing the elements of the most common computer crimes. In addition to the harmonization of substantive and procedural criminal law of the member states, the Convention also provides for a number of practical measures of an international nature. Special attention is paid to supporting the investigation of computer crimes and criminal proceedings related to this category of offenses. At present, the Convention on Cybercrime has been ratified by more than 50 states, including non-European countries (Australia, the Dominican Republic, Israel, Canada, Mauritius, Panama, the United States, Sri Lanka, and Japan). The Republic of Bulgaria has also ratified this Convention.

However, the Convention on Cybercrime does not establish a transparent mechanism for interaction between law enforcement authorities for the prevention, detection, and investigation of computer crimes. It primarily concerns computer crimes of a regional nature (initially applicable only to European states) and reflects the interests of NATO member states. It also contains legal gaps and conflicts (for example, issues related to the collection and presentation of electronic evidence, the liability of hosting providers, etc.).At the Tenth United Nations Congress on the Prevention of Crime, held from 10 to 17 April 2000 in Vienna, the Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first Century was adopted. Paragraph 18 establishes that UN member states commit to strengthening their capacities to prevent, investigate, and prosecute crimes related to the use of high technologies and computers (Vienna Declaration).

The Twelfth United Nations Congress on Crime Prevention and Criminal Justice (Salvador, Brazil, 12–19 April 2010) adopted the Declaration on Integrated Strategies in Response to Global Challenges: Crime Preventionand

Criminal Justice Systems and Their Development in a Changing World**.** This declaration proposes that the Commission on Crime Prevention and Criminal Justice consider convening a meeting of an intergovernmental group of experts to build the capacity of national authorities to counter cybercrime, including prevention, detection, investigation, and prosecution of such crimes in all their forms, as well as to strengthen the security of computer networks (Congress, 2010).At the subsequent Thirteenth United Nations Congress on Crime Prevention and Criminal Justice (Doha, 2015), the Doha Declaration reaffirmed international cooperation in combating computer crime and in creating a secure and resilient cyber environment, as well as in preventing and suppressing criminal activities carried out via the Internet. With regard to the development of criminal-law foundations for combating computer crime, the declaration focuses on specific categories of computer crimes requiring special attention from the international community: identity theft, recruitment for the purpose of human trafficking, and the protection of children from exploitation and abuse via the Internet.

Returning to the issue of countering computer crime in the context of developing criminal-law foundations to combat this negative social phenomenon, the adoption of a United Nations Convention on combating computer crime, in the author's view, is a long-overdue necessity. At present, a certain degree of politicization and alignment of the Council of Europe Convention on Cybercrime (EU, 2025) in favor of the United States, the European Union, and other developed countries (Australia, the United Kingdom, Canada, Japan, etc.) has led to the situation in which many developing countries in Latin America, Africa, and Asia are seeking a fair alternative to ensure their cybersecurity and protect their national interests by creating their own regional international legal instruments.

Conclusions:-

It is particularly important to note that the international measures undertaken to protect against cybercrime still insufficiently address issues related to cybersecurity in the field of food supply, especially with regard to food self-sufficiency and food security. When preparing such legal and regulatory instruments, it is necessary to take into account all problems of a political, legal, procedural, and organizational nature—particularly those that hinder the activities of international judicial institutions. These include, for example: interference in the information space of sovereign states and the jurisdiction of national courts; differences in the criminal legislation of foreign states regarding the differentiation of liability for computer crimes; the lack of relevant multilateral and bilateral agreements between states on mutual legal assistance in criminal matters, including with regard to the extradition of cybercriminals; and the unwillingness of a number of countries to recognize the jurisdiction of international judicial institutions.It should also be noted that, in the absence of a universally recognized United Nations international instrument, the criminal-law framework for combating computer crime remains bilateral or multilateral in nature.

References:-

1. KOPCHEVA, M., 2006 Kompyutarniprestapleniya. Sofia: Sibi.
2. Convention On Cybercrime**.** [online] Viewed 30 Nov. 2025. Availablefrom: https://rm.coe.int/16802fa426.
3. VIENNA DECLARATION onCrimeandJustice: MeetingtheChallengesoftheTwenty-firstCentury. [viewed 09 nov. 2025]. Availablefrom: https://digitallibrary.un.org/record/422888?ln=ru&v=pdf.
4. TwelfthUnitedNationsCongressonCrimePreventionandCriminalJusticeSalvador, Brazil, 12-19 April 2010. [viewed 09 nov. 2025]. Availablefrom: https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/In-session/ACONF.213L.6/L6_E_rev_16_04_10.pdf
5. ThirteenthUnitedNationsCongressonCrimePreventionandCriminalJusticeDoha, 12-19 April 2015 [viewed 09 nov. 2025]. Availablefrom: https://docs.un.org/en/A/CONF.222/L.6
6. UN Manual on the Prevention and Control of Computer-Related Crime . [viewed 09 nov. 2025]. Available from: Manual_ComputerRelatedCrime%20(1).pdf
7. Proposal for a Council Decision ontheconclusion, onbehalfoftheEuropeanUnion, of the United Nations Convent ion against Cyber crime; Strengthening.
8. InternationalCooperation for Combating Certain Crimes Committed by Means of formation and Communicatio ns Technology Systems and for the Sharing of Evidencein Electronic Form of Serious Crimes. [viewed 09 nov. 2025]. Available from: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52025PC0417