

*Кисорець Є.,*  
здобувач ступеня вищої освіти бакалавра  
Національної академії внутрішніх справ  
**Консультант з мови: Романов І.**

## **THE DEFINITION OF CYBERCRIME**

Cybercrime is expressed as a horrible committed contrary to a group of individual or individual by the help of new technology for instance chat room, email, internet with the crime decide of helpfully producing emotional harm, physical and mental. The purpose of computer-dependent technologies is to committing an offensive crime over cyberspace. Different kinds of cybercrimes occur such as identity theft, cyber extortion, online scam, cyberbullying, copyright infringement, and online fraud [1]. Besides, it is necessary to know that cybercrime can exist in different angle or schema for example online website, social media platform and email.

Cybercrime has developed into involvement for public code and has been investigated by the use of crime theories, situational factors, and individual factors. Moreover, the internet does not stand alone to give internet connection for a laptop so, it is useful to see the different device connected to the internet to deliver and acquire data like cyber threats and cellular objects .Nowadays the trends in information and communication technologies have raised the speed of personal information exchange, storage, share, and processing to remarkable level.

In the new world, cybercrime is considered destructive. It is an act for which penalized is charged upon persuasion. A few soft of cybercriminals are noted as blockages are these persons who are virus designer. Hacker area person who discover other laptop structure for education, pranksters are humans who try to attack others. Harassment is a cyber-despotic that happens with the aid of the internet. Computer junk mails refers to unsolicited industrial classified ads dispensed online by using email, that can from time to time raise viruses and anther tools that affect the computer and the restriction of cybercrime is relay on desirable evaluation of their behavior and taking off their affects over extraordinary degrees of society [2]. Therefore, cybercrime appreciation in the modern era and their consequence over society in the coming traits of cybercrimes ware expressed.

The number of cyber-crimes exists all over the world will catch a top-level to obtain money in an unauthorized way. Whilst the relationship between crime and technology is not known, the studies suggest that crime is transposed since the 1990s, gaining new directions and establishing an array of recent obstacle and aids on policing [3]. The characteristics of online criminal activity mean the capability criminals have needed an

international reach in investigating illicit intrusions into digital networks to collect information, demolish websites or perform distributed retraction of service attacks.

All electronic objects which can combine within the internet and capable to deliver and receive information or data could be classified as a computer when considering cybercrime. Cybercrime also involves non-financial misdeed, for example creating and disseminate data that have a virus on other device or computer or releasing confidential company information over the internet. Conceivably, the most dominant type of cybercrime as identity theft; by criminals involve the internet to access personal data or file from other sources and this can take place in phishing and phrasing.

The word cybercrime has been used to explain a large variety of criminal activities that are internet dependent. Cybercrime is explained by totally different people, for instance, national security authority, policeman, criminologist, technical consultant and unprofessional persons. The explanation of cybercrime is few settled once as a result of it is outlined more generally or narrowly. Merely place, the definition of cybercrime ought to not be constricting as a result of the advancement of the technology can virtually definitely be faced to an alteration of cybercrime that is why, many like to suppose of cybercrime as a never-shifting customary of behaviors. Consequently, there is no constant definition of the word cybercrime, and also there is no local and global consensus on what cybercrime means. Because of the above-explained reason the universally accepted definition of cybercrime residues elusive. Below is some example of the definition of the cybercrime:

- Cybercrime is an activity that area unit either misappropriate or thought of eliciting by sure groups and that will be accompanied through worldwide connected electronic device or networks.
- A criminal activity which is dedicated using a laptop and desktop that befalls above the internet;
- All types of crime that has been happened by using a network or computer system in a network or computer system or against a network or computer system. In standard, it includes every crime able to taking place in an electronic environment;
- It can be any cyber-relay crime happened merely through the use of information communication technology and technology-based device, whatever the devices are a unit each the target for committing the crime, and the vector of cybercrime; or cyber-enabled which area unit ancient crimes which might hyperbolic or raise in scale or increase by the use of laptop,

computer network or other forms of information communication technology;

- Refers to strategies by those computers or different electronic devices area unit accustomed to perform criminal activities and cause damage to others.

Even though nearly individuals explained cybercrime inversely, they altogether agree on the substantial role which networked computer technologies play an indefensible role in the committing of these kind of criminal activities. Different activities which is considered as cybercrime has been categorized is fallen under the umbrella of the networked system.

#### **Список використаних джерел:**

1. Rana A. Shalhoub, Huda Ayas Enforcing Cybersecurity in Developing and Emerging Economies: Institutions, Laws and Policies. Edward Elgar Publishing, 2017. 272 c.

2. Majid Yar, Kevin F. Steinmetz Cybercrime and Society. SAGE, 2019 p. - 368 c.

3. Brian D. Loader, Douglas Thomas Cybercrime: Security and Surveillance in the Information Age. Routledge, 2013 p. - 320 c.

***Коваль Р.,***

здобувач ступеня вищої освіти бакалавра

Національної академії внутрішніх справ

**Консультант з мови: Гіпська Т.**

### **MAIN ROLE OF INTERNATIONAL ORGANIZATIONS IN COMBATING CYBER CRIME**

The growing statistics of cybercrime demonstrate the ineffectiveness of cybercrime mechanisms, as the cross-border nature of high-tech crimes makes it impossible to combat them effectively within national legal systems alone. That is why, since the end of the twentieth century. States have begun the process of cooperation within various international organizations to counter the threats posed by the latest technologies.

Central to this process is the United Nations and its specialized agencies. The United Nations Office on Drugs and Crime, which runs the Global Program on Cybercrime, and the Intergovernmental Panel on Open-ended Crime composition on cybercrime (Open-ended Intergovernmental Expert Group on Cybercrime). UNODC promotes long-term and sustainable capacity-building in the fight against cybercrime by supporting national structures and actions.

Another UN institutional mechanism is the Commission on Crime Prevention and Criminal Justice, established by ECOSOC Resolution