ISSN NO: 2770-0003
Date of Publication: 06-04-2023

Cybercrime As A Threat to Society

Akmaljon Kabulovich Artikov
Head Of The Main Hr Department Ministries Of Defense Of The Republic Uzbekistan
E-mail artikov@inbox.ru

Annotation: this article provides an overview of the growing number of cybercrime to date, as well as the fight against them.

Key words: cyberattack, cybercrime, hacker, network, information, web pages, social network, virtual space, computer, programs.

Cybercrime is crime in the so-called virtual space. Virtual space or cyberspace
define as an information space modeled by a computer, in which there is information about persons, objects, facts, events, phenomena and processes, presented in mathematical, symbolic or any other form and in the process of moving through local and global computer networks, or information stored in the memory of any physical or virtual device, as well as other media specially designed for their storage, processing and transmission.

A crime committed in cyberspace is a culpable unlawful interference with the operation of computers, computer programs, computer networks, unauthorized modification of computer data, as well as other unlawful socially dangerous actions committed with or through computers, computer networks and programs.

Cybercrime is a generic concept that covers both computer crime in the narrow sense of the word (where the computer is the subject, and information security is the object of the crime), and other attacks, where computers are used as tools or means of committing crimes against property, copyright, public security or morality (for example, computer fraud, etc.). The latter are often referred to as “computer-related crimes”.

Adjacent to cybercrime are some actions aimed at maintaining the conditions for its existence and development (using e-mail for communication, creating your own websites aimed at spreading criminal ideology, as well as sharing criminal experience and special knowledge).

It seems that it is necessary to distinguish between cybercrime as a legal category and cybercrime as a social phenomenon.

As you know, cybercrime knows no state borders. Perhaps, in order to develop the most appropriate standard definition, one should refer to the experience of international organizations. One of the serious steps aimed at resolving this problem was the adoption by the Council of Europe on November 23, 2001 of the Convention on Combating Cybercrime.

Considering the complexity of the problem, the Council of Europe prepared and published a draft Convention on the Suppression of Crimes in Cyberspace as early as the beginning of 2000.

This document was the first international agreement on the legal and procedural aspects of the investigation and prosecution of cybercrime.

The Cybercrime Convention provides for coordinated actions at the national and interstate levels to suppress unauthorized interference in the operation of computer systems, illegal interception of data and interference in computer systems.

Cybercrime can be defined as a subcategory of computer crime.

The term refers to crimes committed using the Internet or other computer network as a component of the crime.

Classification of cybercrime

The Council of Europe Cybercrime Convention speaks of four types of “pure” computer crimes, defining them as crimes against the confidentiality, integrity and availability of computer data and systems:

Illegal access - (illegal intentional access to a computer system or part of it);

Unlawful interception - (illegal intentional interception of non-public transmissions of computer data to, from or within a computer system);

Interference with data - (unlawful damage, deletion, violation, alteration or suppression of computer data);

ISSN NO: 2770-0003
Date of Publication: 06-04-2023

Interference with the system - (serious unlawful obstruction of the functioning of a computer system by entering, transferring, damaging, deleting, disturbing, altering or suppressing computer data).
It is these four types of crimes that are actually "computer", the rest are either computer-related or computer-facilitated crimes. At the X UN Congress on the Prevention of Crime and the Treatment of Offenders at the symposium on crimes related to computers and computer networks, the concept of cybercrime was considered from the point of view of two aspects:
Cybercrime in the narrow sense (computer crime): any illegal act committed through electronic transactions, the purpose of which is the security of computer systems and the data processed by them.
Cybercrime broadly (as computer-related crime): any wrongful act committed through or connected to computers, computer systems or networks, including the illegal possession and offering or dissemination of information through computer systems or networks.
In addition, several categories of cybercrime were proposed at the X UN Congress.
One of the classifications implies a division into: violent or otherwise potentially dangerous (physical threat, cyber harassment, child pornography, cyber terrorism) and non-violent crimes (wrongful trespass in cyberspace, cyber theft, cyber fraud, advertising of prostitution services on the Internet, drug trafficking with using the Internet, gambling on the Internet, money laundering through electronic transfer, destructive cybercrime, other cybercrime).

Methods for combating cybercrime

An effective fight against cybercrime presupposes an adequate clarification of the specifics of the reasons for its growth. In general, criminal manifestations have a single causal complex, which is based on the deepest and most acute deformations in society in all its spheres and levels, from the global global to the individual-personal.
These are such deformations that, firstly, express the injustice of the social structure, open up scope for the arbitrariness of some subjects to the detriment of others; secondly, they infringe on the rights and freedoms of citizens, and thirdly, they lead to dehumanization and inferiority of the social status and mentality of a part of the population.
This is due to the fact that, although cybercrimes are committed with the help of computers, computer systems and networks and in a virtual environment, nevertheless they go to the physical level and cause material harm, and, therefore, encroach on real legal relations, affect the interests of specific people, bring negative consequences. In this regard, the existing norms of administrative and criminal laws in force on the territory of the Republic of Uzbekistan are also applicable to these crimes.

Conclusion

Cybercrime and cyberterrorism are an objective consequence of the globalization of information processes and the emergence of global computer networks.
With the growing use of information technology in various fields of human activity, their use for the purpose of committing crimes is also growing.

The need to protect against cybercriminals is obvious. It is desirable that the problems of combating cybercrime be solved at the state level, and work should be carried out everywhere to clarify the protection against cybercriminals. Our safety is in our hands!

List Of Used Literature:

1. http://mvnik.ru/images/informatika/kiber.pdf
2. http://www.myshared.ru/slide/439133/#
3.http://ppt-online.org/4680
4. http://www.kaspersky.ru/downloads/pdf
5. http://www.myshared.ru/slide/439133/#
6. http://www.plusworld.ru/daily/kiberprestupleniya-v-rossii-vishli-na-industrialniy-uroven.