British Journal of Global Ecology and Sustainable Development
Volume- 39, April 2025
ISSN (E): 2754-9291

GLOBAL THREATS AND SECURITY ISSUES IN CYBERSPACE

Dilafro'z Eshankulova Alisherovna
Senior Lecturer of the Department of Social Sciences
Faculty of International Journalism Uzbekistan State
World Languages
dilafruz84_84@mail.ru

Sharifjonov Jalilbek Anvarovich
2nd Student of Political Science Faculty of International Journalism
Uzbekistan State World Languages
jalilbeksharifjonov@gmail.com

Abstract:
This article describes the development of media space in the era of globalization, the increase in information attacks and how this affects the life of society. Crimes committed in cyberspace, in which widely disseminated ideologies, harmful ideas are expressed in the national interests of states, social institutions in society, inviolability of individuals, and moral damage are indicated by specific facts and statistics. What measures the states take to maintain cybersecurity, the laws adopted are mentioned.

Keywords: Cyberspace, cybersecurity, cyberterrorism, fundamentalism, religious extremism, cyberspace, mass culture, soft power, national content, cyberstalking, doxxing, manipulation, globalization, computer networking.

Introduction

Living in the age of globalization, we have achieved great achievements in technology, science. In particular, the intense development of modern technologies has conquered all the spheres that exist in society and created various comforts for human life. These technologies provided so many opportunities that economic, political and ideological forces also made extensive use of it. Indeed, the intensity of globalization has shown that humanity is not yet ready for this wave, bringing negative vices and global issues along with many achievements. In particular, the media space, which concentrated all the amenities in itself, became the main "front line". Now, ideological attacks rather than armed ones move to the main plan, and the hegemonic states, various societies, groups, sects actively move in the media space to realize their goals. To date, "mass culture", "soft power", "fundamentalism", "religious extremism", "cyberterrorism" and a number of other cybercrime, extremist ideologies have become trending words that all develop in cyberspace, endangering the national interests of states. It is the issue of cyber security that is one of the main topics put on the agenda in all states. Cybercrime is broad in scope, capable of causing moral and material harm. The proof of my word is that as a result of cyberattacks in the United States of America alone, 452.3 billion material damage was inflicted on the state[1].

Cyberspace is a virtual environment formed through the internet and other digital networks. The term was originally coined by Canadian writer William Gibson in his 1982 story “Burning Chrome”. The writer also uses the term in his techno-utopian fantasy trilogy, “Neuromancer”. In the work, cyberspace is defined as a collective hallucination, a kind of delusional form. The processes that take place in cyberspace, combined with the psychological manipulation of people, especially young people, pose a huge danger to their personal inviolability. There are only psychological aspects to influencing the minds of young people. The electronic mass communication revolution entered youth thought with great force. Because of virtual life, for example, in the land of South Koreans, more than fifteen to sixteen years ago, data showed that hundreds of young people did not speak to their parents. As a result, we must say that in some young people of mainly developed countries, indulging in humanity, occultism, sadism, suicidal behavior has become a common phenomenon[2].

As young people use many platforms in cyberspace, they collide with informative manipulations. Some groups seek to change the social, political and religious views of young people by disseminating fake information on social networks. A vivid example of this is the leaked social media material, propaganda of extremist groups such as “Hizb ut tahrir” (free Islamic Party), Al-Shabaab, ISIS, and Jehovah's Witnesses, which led many people to go to their ranks and join them and become victims. In addition, manipulative technologies such as “clickjacking” and “clickbait” are widely used to distract young people This is made possible by the fact that technalogies are misinformed in a sensational way or in order to attract attention. The system of social networks is structured in such a way that, through computer algorithms, the user displays a certain amount of information-content more, depending on his interest.

One of the most common types of cybercrime is cyberbullying which is done by forcing a person to do a certain job by threatening, shaming them over the internet. There are several types of it. "Doxxing" (dissemination of personal information) is also a focus of cyberbullying, undermining the personal inviolability of a social network user by disseminating personal information (address, telephone number, activity). "Cyberstalking" (online harassment) is used to cause moral harm to human activities. In particular, actions such as constant monitoring, writing uncomfortable messages interfering with privacy through anonymous accounts are committed. For example, almost 42% of children are abused in positive networks. In recent years, surveys have found that mostly teenagers between the ages of 10-17 have been victims of this type of crime. 56% of such cases were observed in chats of social networks[3].

[1] https://www.statista.com
[2] Siyosiy madaniyat [Matn]: o’quv qo’llanma / D.S. Muitov.- Tashkent: “BOOK TRADE 2022”, 2023. – 37-38 b.
[3]https://www.annapolis.gov/908/Facts-About-Cyberbullying

Cyberterrorism is very widely used in the implementation of political, strategic goals. Focusing on the lexical meaning of cyberterrorism, deliberate attacks on information, computer systems, computer programs and information that are politically based, expressed in the use of force by subnational groups or secret agents against non-military targets[4]. This type of terrorist action is carried out through the internet and digital technologies, mainly directed against the government, critical infrastructures and the public. For example, on may 12, 2017, attacks were launched worldwide with the "WannaCry" virus. The virus damaged more than 230,000 computer systems in 150 countries and caused financial losses of approximately $4 billion. "WannaCry" also had a significant impact on the British National Health Service (NHS). About 20,000 medical appointments were cancelled due to hospitals and clinics being cut off from the system. In June 2019, Russia recognizes that its power grid is "vulnerable" to cyberattack by the United States. According to The New York Times, United States cybersecurity hackers deployed malware that could disrupt Russia's power grid[5].

Scholars such as Ali Dehghantanha, Sadie Creese, Jason Healey and Nazli Choucri have made significant contributions to the field of cybersecurity through their extensive research. Their work explores not only the historical evolution of cyberattacks but also the underlying factors that facilitate their occurrence and the mechanisms that can aid in their prevention. By analyzing past cyber incidents, these scholars provide valuable insights into the formulation and adaptation of contemporary cybersecurity strategies. Their research spans key areas such as the enhancement of cybersecurity policy, interstate relations within cyberspace, the development of international frameworks for addressing cyber threats, and the design of political strategies to counteract cyber conflicts. A common thread across their work is the emphasis on the integration of artificial intelligence as a powerful tool in detecting, analyzing, and mitigating cyberattacks, thereby reinforcing global cyber defense capabilities.

At a time when the geostrategic struggle of the States is going on, there is a lot of attention on the issue of cybersecurity, and rapid reforms are being carried out in this regard. In Germany, for example, since 1997, there has been a federal administration investigating materials that could harm young people. The scope of its powers includes the creation of a list of impure and not allowed for sale products (Media, books, videos and computer games) and measures to obtain violations in this direction. The legislation of such countries as the current Netherlands, Switzerland, Denmark, Japan, China, Uzbekistan, Russia provides for criminal liability for the dissemination of information that can adversely affect the psyche and spiritual growth of young people[6]. Since media space is considered the main center in the spread of various ideologies, "mass culture", the need to create strong national content is put on the agenda. Naturally, under the

[4] Axborot texnalogiyalari atamalarining izohli lug'ati. – Tashkent: "Kafolat print company" nashriyoti, 2023. - 282 b.

[5] https://uzpedia.uz/pedia/kiberterrorizm

[6] Qodirova Z. Axborot xurujining yoshlar dunyoqarashiga ta'siri. To'plam. Yoshlarni axbarot-psixologik xurujlardan himoya qilish texnalogiyalari: nazariya va amaliyot. -T.: O'zMU, 2012. 151-bet

guise of "mass culture", the dissemination of the ideas of moral decay and violence, invidualism, egocentrism, the achievement of wealth at the expense of reason, the centuries-old traditions and values of other peoples, infertility to the spiritual foundations of a lifestyle, threats aimed at their rudeness, do not concern a person[7]. In this matter, the president of the Republic of Uzbekistan SH.M.Mirziyoyev's decision dated March 26, 2021: "there is no integrated system in the organization of spiritual and educational processes, there is not enough organizational and practical and research work on the protection of our people, especially young people, from spiritual threats" public organizations, civil society institutions, media and social cooperation of the private sector in this direction have not been[8]. This entails increasing media literacy in society, forming strong national content, protecting the immunity of individuals in cyberspace, and implementing rapid reforms in cybersecurity. On February 25, 2022, the Cybersecurity Act was passed by the Legislative Chamber of the Oliy majlis of the Republic of Uzbekistan. This law regulates relations in the field of cybersecurity. The law states that the priority tasks are to protect the interests of the individual, society and state in cyberspace from external and internal threats, cooperate with international organizations in this area, conduct research in the field of cybersecurity, and organize monitoring. At a time when information attacks are affecting the minds of young people, such reforms should cover the entire layer of society. Especially in schools, knowledge in this area should be passed as a science or in addition to certain disciplines, combined with the formation of mediasavodkhanism in young people, in which a strong "immunity" should be formed in relation to negative information. In the formation of this "immunity", it will be advisable to attract not only science teachers, but also specialists in the field, ensuring their active participation. "Adolescence" is considered the most influential period, and mainly young people are victims of spiritual and ideological threats. It is in school education that they develop skills such as critical-analytical thinking, information analysis, the formation of psychological stability, strategic thinking, which serve as a defense to them and reduce, prevent the risks mentioned above. In addition, in the age of technologists, since all individuals have the opportunity to participate in cyberspace using modern gadgets, such activities of young people, especially schoolchildren, are controlled by both teachers, officials and their parents. Because the mass culture and ideologies that are widely spread in the media space quickly settle into their lives and have a strong influence on the circle of thinking. Looking at the other side of the issue, poisoning in cyberspace is most often observed not only in young people, but also in older people. Since media literacy, political culture, legal knowledge are not sufficiently formed, many cases of damage from cyber attacks are observed. To fill such a gap, issues such as giving constant recommendations by specialists in all regions, increasing the effectiveness of legal assistance to citizens in these issues, moving these activities to the media space, forming a strong "national

[7] Yuksak ma'naviyat – yengilmas kuch. I.Karimov. – T.: <<Ma'naviyat>>, 2009. – 117 b.
[8] Siyosiy madaniyat [Matn]: o'quv qo'llanma / D.S. Muitov. - Tashkent: "BOOK TRADE 2022", 2023. – 59 b.

content" take an important place. On the issue of "national content", it is difficult for socio-political institutions, drumming organizations and the media to effectively establish cooperation, to do the same, to use the ideas of our national values, traditions. In a legal-democratic state, such measures serve as an important tool in the formation of civil society, in maintaining the safety and stability of society.

References

1. https://www.statista.com
2. Siyosiy madaniyat [Matn]: o'quv qo'llanma / D.S. Muitov.- Tashkent: "BOOK TRADE 2022", 2023. – 37-38 b.
3. https://www.annapolis.gov/908/Facts-About-Cyberbullying
4. Axbarot texnalogiyalari atamalarining izohli lug'ati. – Tashkent: "Kafolat print company" nashriyoti, 2023. - 282 b.
5. https://www.security.com/feature-stories/wannacry-lessons-learned-1-year-later
6. https://uzpedia.uz/pedia/kiberterrorizm
7. Qodirova Z. Axbarot xurujining yoshlar dunyoqarashiga ta'siri. To'plam. Yoshlarni axbarot-psixologik xurujlardan himoya qilish texnalogiyalari: nazariya va amaliyot. - T.: O'zMU, 2012. 151-bet
8. Yuksak ma'naviyat – yengilmas kuch. I.Karimov. – T.: <<Ma'naviyat>>, 2009. – 117 b.
9. Siyosiy madaniyat [Matn]: o'quv qo'llanma / D.S. Muitov. - Tashkent: "BOOK TRADE 2022", 2023. – 59 b.