

# Formation of Cyber Space, Protecting Youth From the Danger of Cyber Extremism

Mukhamedzhanova Lalikhon Ashuraliyevna, Kadirova Dilbar Salihovna, Agzamova Nilyufar Shuhratovna, Tulaev Avaz Ilhamovich, Rajabov Shukhrat Sheraliyevich, Alimov Sardor Komilovich

*Abstract: Nowadays, modern information technologies, along with enhancing human communication capacities, have led to global socio-economic, political change. This, in one sense, has led to the deepening of the spiritual crisis, the risk of loss of national cultural identity. Therefore, "cyber-stringism", which is of great concern to the general public, which sometimes affects the general public and is sometimes concerned with the socio-political change of the individual, the state's greatest competitor, is now recognized as the biggest problem worldwide. Therefore, it is time to pay special attention to the negative impact of "cyber-capitalism" on the moral life of human beings and society during the era of globalization.*

## I. INTRODUCTION

The second half of the 20th century and the advanced technology at the turn of the 21st century have highlighted the issues of globalization and the informational social structure, which have been permanently discussed in recent years. The world's present-day landscape is even more vivid and informative through information and communication technology, but it is also a terrifying experience. In the era of globalization, information security in cyberspace is one of the most important tasks. The cyber crashes taking place in this process are increasingly threatening humanity. This is cyberspace cyberspace, cyber-terrorism and other cyber-cyber threats. Shavkat Mirziyoev, President of the Republic of Uzbekistan, addressed the 72nd session of the UN General Assembly on "The threat of terrorism in the world, especially in recent years, shows that the method of combating terrorism is not justified. In this case, it is often restricted not only to the major causes of threats, but also to the consequences of threats. I believe that the roots of international terrorism and extremism are, among other things, ignorance and intolerance. "

## II. LITERATURE REVIEW

**Revised Manuscript Received on July 05, 2019.**

**Mukhamedzhanova Lalikhon Ashuraliyevna**, Ph.D. in Philosophical Sciences, Professor, National University of Uzbekistan (NUU), Tashkent, Uzbekistan

**Kadirova Dilbar Salihovna**, Ph.D. in Philosophical Sciences, Associate Professor, National University of Uzbekistan (NUU), Tashkent, Uzbekistan

**Agzamova Nilyufar Shuhratovna**, Ph.D. in Philosophical Sciences, Associate Professor, National University of Uzbekistan (NUU), Tashkent, Uzbekistan

**Tulaev Avaz Ilhamovich**, Senior Teacher, National University of Uzbekistan (NUU), Tashkent, Uzbekistan

**Rajabov Shukhrat Sheraliyevich**, Teacher, National University of Uzbekistan (NUU), Tashkent, Uzbekistan

**Alimov Sardor Komilovich**, Teacher, National University of Uzbekistan (NUU), Tashkent, Uzbekistan

Online cybercrime and memberships by people , Protect any online service that is in the virtual world , Protect America from the threat of cyber-terrorism , virtual world cyber wars in South African countries , cybercrime and their legal analysis, analysis of Zanzibar law , Preparing a cyber security consultation plan and to take steps to prevent it , An analysis of online crime prevention models , cybersecurity in Europe: antipublikativ management and practice and other kind of researches have been conducted in this field.

## III. RESEARCH METHODOLOGY

Humanity experiences a period of revolutionary change in the field of information. There is a general informational community in the world. The basis of these changes lies in the fact that the most modern and effective means of information transfer, transmission and distribution of information on telecommunication and computer technologies are born. As a result, the 21st century is recognized as the age of an information society. Internet is his weapon.

The cyberspace is a global set of virtual computer networks in cyberspace. Kibermakon has been expanding and improving since 1990, as a reality that represents the field of communication that is being implemented through computer networks. The Canadian writer William Gibson wrote in his 1982 story about the "Sojeenie Chrome" (The Burning Chrome). Later, Gibson used the techno-utopian trilogy "Neuromancer" ("Nervous Sculptor", "Nervo-Sacinitel"), graduated in 1990.

## IV. ANALYSIS AND RESULTS

The war of the present-day era is accomplished by using cyber weapons in the information space. Extremist and terrorist forces are widespread in their use of the Internet and cybercrime to carry out their actions without any weapons, simply by impinging on the minds of the people, by influencing their morality. The main feature of extremism is the promotion of contradictory views of the values, morals and people's moral values, and the tendency to critical thinking and action.

Extremism is a destructive ideology that is crucial in politics, loyalty to harsh measures, and inciting disorder, disobedience to citizens, and inciting terrorist movements. Extremists in extremes often refuse to agree, negotiate and negotiate. All these actions



will be aimed at performing acts that are contrary to morals. For example, the actions of extremists lead to the loss of a person's internal "I", which leads to humiliation in the people, such as hatred, desires, misery. Such crises will result in a sharp decline in the moral level of the majority of the population, and increase the extraordinariness that is being pursued by extremists in opposition and dissent. In these situations, sharp interventions for individuals and organizations have become the only opportunity to have a clear impact on the situation, especially if the revolutionary situation or the civil war in the country continues to be related to "forced extremism." Scientists who are well-acquainted with this topic say, "It is a realistic thing to understand and understand the complexity of extremism. In the context of the conflict - a solid form of conflict resolution. However, "extremist" or individuals and groups in this category are "normal" or "traditional": they are always subjective and political. VD Trofimov, Coordinator of the People's Rights Protection Movement, said: "Extremism is not just a politically-connected phenomenon, it involves all forms of human activity: extremism is the ideology of extreme measures to be taken to exploit any sphere of influence," he said.

Today, with the dissemination of ideas in some media networks, negative tendencies such as intimidation, violence, and cruelty are increasing. As a result, cyber threats, such as cyberspace and cyber-terrorism, have become a new space in the world of information and extremism, in other words cybercrime. If we pay attention to the geopolitical essence of conflicts and clashes in Afghanistan and some Arab countries, we see that they are actually getting stronger because of the growing cyberattack among different forces in the world. This is now becoming an important fact of providing information security and upbringing harmoniously developed generation, and preventing attacks on their ethical and aesthetic thinking. For example, western individualism is widely promoted through cyber space, and the world's young people have left their traces in the mind and heart of ethical aesthetics. F.Muhamedzhanova describes this idea as follows: "It is important to note that mass media in our country are reporting on such threats, in particular, of the harmful effects of mass culture. In some of them, the news was quickly analyzed by the outspoken tactics of absorbing ideas on "destructive cults", parotatal and neo-natian zhuzes into young people who quickly adopted the information.

While ethnic integration has accelerated on the Internet, there have been some disruptions and chauvinisms that existed in the human societies for centuries, from real-time to virtual worlds, and have been used as a weapon of ideological-psychological warfare in the global network, which is still under development.

If we look at the phenomenon in cyberspace, we see that it is beautiful from the outside, and the beauty of its originality

leads people to desecration. The original beauty is determined by the truth, truthfulness and reality of the event. The reality and reliability of the events taking place on the cyber space are very low. For example, in some cases, photographs posted by human beings are not used in real-time on social networks to interact with other people's photographs, the information they provide is unreliable, and information about any movie heroes, stars' deaths, or immoralities is unreliable; .

Internet space is expanding every minute. Thousands of new sites are being created every day in the world. Among many portals, you can see music and movies, sites dedicated to religious fanaticism, and "infidels" to extremist extremism and warfare. Today, the need for information security has become an integral part of life. Information has become not only a valued object, but also an effective tool for manipulating people.

The information contained in the hands of extremists is a dangerous weapon. Today, crimes committed by extremists, including cyber-stricken extremists, have come out of speculative situations and have become a problem that creates negative emotions that affect the peace of the world and their thinking. They became not only sources of threat to the national security of our country, but also to the whole of humanity.

Given that we can not imagine today without information technology, it is difficult to understand how dangerous this place is. True, these technologies have become the greatest discovery of human beings, but we all know that human tendencies are worse than good in the minds of the people. This place is very rich in news. No one knows exactly how accurate these reports are. Only this is how people accept it with the "beauty" as it is. The extremist forces who spread such information widely use this Internet space to carry out their own plans, as a result of which there are adverse changes in the ethical thinking of young people in cyberspace.

Special attention is paid to the problem of cyber-stricken and cyber-terrorism, which is considered to be a humane danger, as a new and unsearchable crime scene. Cyber-attackers are able to obtain secret information by illegally destroying sites. The Kibermakon religion does not go too far. Forms of these processes are reflected in the following forms: communication, information, training, experience, practice, missionary, marketing, medicine and others.

According to A.Yu.Pidjakov, "Cyber-Stremism is one of the many common cyber-stereotypes. Its objectives include political or economic crisis, sabotage, military or civilian assets, and political theft of resources. At the same time cyber-stammers are primarily

interested in eradicating moral and aesthetic reasoning. The person who has lost interest in beauty and beauty is no different to manqurt. Today, cybercriminals are the only people who have Internet access because they are not human - they see what they want. The first reason for this is interest, first of all interest, and then gradually moves on in his own way. As a result, one person becomes a victim of cyberspace. Fear of superficiality and uncertainty, or a lack of innovation in the interest of human beings, is a characteristic feature. That was the first time people used technology and technology. However, with the help of these technologies, human civilization is developing. It is recognized that the most important means of doing so is becoming a reality through the Internet.

The idea that the Internet, which is a popular means of communication, as a place where cultures collide, is the cause of the mass culture and the likeness of the "Trojan horse," which spreads its inaccessibility. As you know, any developmental product can be used for two purposes - good and evil. In particular, it is possible to see that the history of humanity has existed since ancient times, with the noble ideas and teachings that call for human perfection, the higher goals, and the everlasting struggle between evil and harmful ideas.

The cyberwar and the ideological expanse are striking with the economic blockade and the threat to our national values. Extremism has begun its new phase, namely, cyber-sterimism. So, what are the contemporary views of cyber-strickenism? Another problem with cyber threats is that in many cases, it is trying to dispel the country's stability through cyber attacks, using the ideology's polygons, which, like most economic crises, unemployment and poverty corruption, For example, the political processes in the Egyptian Arab Republic once again prove that the prospects of these processes are related to the uncertainties. We are all witnesses of the "colored revolutions" that took place in Ukraine, Kyrgyzstan, in the states of the Western world.

Political scientist Abdukholiq Tashanov states in his research: "Cybercrime - modern information communication is one of the forms of threat to the individual, society and the state, using media technologies. It is widely acknowledged today that terrorist organizations are trying to exploit ICTs for their destabilizing purposes. The world's first large-scale cyber-propaganda industry has been targeted to disrupt the industry. The powerful computer virus called "Stuxnet" attacked Iranian infrastructure facilities, including nuclear power plants and water treatment facilities in 2010. Over the past two years, North Korea has been accused of cyber attacks against South Korea, particularly South Korean banks and virtual offensive international airport Inchkhan. India has accused Pakistan of cyberattacking. Thousands of ethnic minorities have dropped out of Bangalore because of the

rumors that the Pakistani side has posted on the Internet.

Cyber-stammer has its own important policy in the politics and economy, and even developed countries use it as a weapon of illicit weapons. For example, the Antivirus Laboratory, called PANDLABS, has released a ranking of fraudulent Internet penalties over the last five years. In this rating, Nigeria's fraud, Loteria, Mahbuba, Employment Opportunity, and Compensation are ranked high. They are extending the "great fraudstroke" by assimilating people's possessions and stealing their possessions.

## V. CONCLUSION

Cyber-extremism is a growing threat to modern society and a complex public-political task. The security issues of information resources associated with cyber-stringism in the information system are ever stronger than ever. Every year, the number of adolescents admitted to extremist organizations is rising, and many of them are accidentally exposed to extremist networks and do not understand the real consequences of their actions.

Prevention of cyber-strife among young people should be done simultaneously in three areas: legal, acmeological and technological.

- The legal aspect should be reflected in the perfect law in the field of combating extremism. This law takes into account the past and present experience of the universe in general. The cyber-stereotypes need to be aware of the level of responsibility they have received, to promote certain radical views among young people, and to know the inevitability of punishment for such acts. The majority of young people, especially teenagers, are not satisfied with their fate or their role in society, which creates a good foundation for disseminating ideas of extremism and terrorism on the Internet.

- The ecological direction is related to the formation of youth value system. To do so, young people should be able to enter cultural and artistic values and simplify the use of cinema, literature, art and social networking capacities. Speaking of the latter, his essence is to create games and tournaments that are directly linked to human values. It is a legitimate and technologically important measure, because a young man who is unable to distinguish between evil and evil is not just a cyber-strain, but a misunderstanding of society.

The latest and least important aspect of technology is that it is very limited to the youth as a social group. In this area, it is necessary to filter Internet content and access potential potentially dangerous resources. Content filtering can be of three levels: provider, server, and client station. Internet filters are usually unable to work with context, which



requires context filtering. Today it is used by spam-filters.

Cyber Warfare - an artless and fierce battle; defeat his opponent without defeat.

A person can not be free from the society while living in society. It also directly affects the whole work of a person, including his moral appearance, and poses some specific educational and traditional requirements for his behavior. Guarantee of access to information must become a value that is directly linked to national interests, which is directly beyond personal interest. In such circumstances, it may be necessary to prohibit the dissemination of information, the negative impact of society's ongoing social, national, ethnic, discrepancies and disagreements, the propagation of violence and war, pornography, domestic violence, and the detrimental effects of the reputation, there are spiritual-psychological norms based on informal, conscientious, healthy minds and high ideals. The concept of information security is thus a moral and ethical dimension. In a civil society where freedom and personality is a collective, information security systems should be developed. It depends on the political level, professionalism, and, most importantly, the civic position, the sense of belonging to the society, directly and indirectly, of media outlets and service providers. Indeed, the main criterion for maintaining the information-analytical security and the main supporter is a sense of patriotism, patriotism, devotion. Of course, there are specific basics of information security.

First of all, organizational and technical provision. Equipped with modern technology and technology.

Second, to have a solid financial and financial basis. Information - Increasing the interest of employees in the field of security.

Third, the training of talented, full-fledged, intelligent cadres with modern knowledge, capable of managing modern information technologies. This means that the information aggression is increasingly aggravated, individually capable of influencing everybody's mind, broadly capable of solving the fate of society and the fate of the nation, and on the global scale, which guarantees the progress of humanity and determines its progress or deficiency. The development of the principles of management, regulation and use of high-quality information systems is one of the most pressing problems of modern times.

Forming the ability of people to deeply understand national ethical principles and to understand the beauty. Thus, the experience of Uzbekistan in the field of information security is being improved. At the same time, this direct news outbreak, with increasingly improving information technology and its methods and methods, Uzbekistan has been increasingly expanding its access to the most productive and most patriotic methods of that civilization. It is also important that social networks be able to compete with the aesthetically pleasing and competing with other social networks, and the source of the information needs to be explained in a clear, understandable way to the content recipient.

Because of the increasing number of networks in the virtual world, the opportunity to visit and expand is also expanding. That is why they are finding the way to attract their clients by placing their ads. Some social networks use different methods and tools in this regard. It has a negative impact on human consciousness and its ethical and aesthetic culture. The number of temporary users of such sites may increase, but in the future, their number declines. Under the conditions of Uzbekistan, it is necessary to create social-network users based on their age, place of work, territory. The information provided through this information should serve to enhance the consciousness and culture of the people.

## References

- [1] Dearbhail Kirwan, Cybercrime: An Investigation of the Attitudes and Environmental Factors that Make People more Willing to Participate in Online Crime. Dublin Institute of Technology, 2017.
- [2] Santa Barbara, Protecting Online Services from Malicious Activity, University of California, 2016.
- [3] Rogers. Protecting America against cyber terrorism, United States Foreign Policy Agenda, USA, 2017.
- [4] Anna Granova, Marco Slaviero, Cyber Warfare. University of Pretoria, Pretoria, South Africa, 2011.
- [5] Abdalla Haji Faki, Cybercrime and analysis of laws: a case study of zanzibar legal issues, University of Tanzania. 2014.
- [6] James O. Ellithorpe, The Role and Impact of Cyber Security Mentoring. United Kingdom, 2016.
- [7] Ki Hong (Steve) Chon, Cybercrime precursors: towards a model of offender resources, The Australian National University, 2016.
- [8] Professor Dr Toby Seddon, Cyber-security in the European Region: Anticipatory Governance and Practices, The University of Manchester, UK, 2018.
- [9] TIU.Uz, "Indication of Religious Processes in Cyprus" 1 b.
- [10] Kuvatov VI, Primakin AI, Yakushev D.I. Protivodeystvie terroristicheskim i ekstremistskimyu. -Sankt-Petersburg. Rossii: Vestnik Sankt-Peterburgskogo University MVD Rossii № 1., 2015.65 b.
- [11] Trofimov V. D. Extremism (Russian), Provereno 5th of July, 2011. Archives Posted on February 5, 2012 Age.
- [12] F. Mukhamedjonova. Globalization of information and the spirit of youth. -Tashkent. Collection. The technologies of young people's information psychological attack: theory and practice. Materials of the Republican Scientific-Practical Conference, 2012, 32 p.
- [13] A.Yu.Pidjakov Borba s politicizm extremism and terrorism: problemy izucheniya / A.Yu. Pidjakov // Izvestiya VUZov. Pravovedenie. - 2003. - №3. - S.234-244.
- [14] Tashanov A. Destructive ideas and destructive ideologies. - Tashkent. "Turan Zeit", 2015 year; 171 b
- [15] Mogilevtseva O.S., Selenya D.A. Osobennosti prophylactic kiberekstremizma v molodezhnoy srede // Современные научные исследования и инновациями. 2016. [Electronic resource]. URL: <http://web.snauka.ru/issues/2016/12/76097> (data as of 30.09.2017), p.