British Journal of Global Ecology and Sustainable Development
Volume-21, October, 2023
ISSN (E): 2754-9291

SOCIO-POLITICAL MECHANISMS FOR PREVENTING MODERN GLOBAL THREATS AND CYBERSECURITY

Batirov Farxod Avazovich,
Head of the Educational Process-Planning Department, Educational and Methodological Department, University of Public Safety Republic of Uzbekistan
farxod-batirov@mail.ru

Annotation

This scientific article is widely covered from a scientific point of view, which states the following. Socio-political mechanisms for the prevention of modern global threats and cybersecurity in accordance with the priority areas, as well as with the goals and objectives set for the period provided for by the strategy, to develop an action plan including a set of measures in the field of information security and cybersecurity, to develop a multilateral action plan in which each measure highlights the main and other performers approved measures by type of activity, deadlines for implementation and performance indicators, successful implementation of the strategy and similar information.

Keywords: cybersecurity/ cybercrime/ cyberterrorism/ cyberattack/ cyberspace/ cyber threat/ globalization/ operational security/ Information technology security.

Introduction

In order to correctly understand the essence of the globalization process, it is necessary, first of all, to distinguish between the concepts of civilization and culture. Thus, in fact, this civilization has a global scale, since it is a process that expresses the progress of all mankind by its nature. Globalization - (fr. global-general, globus-sphere) is an approach that proposes to carry out all kinds of communication and integration between legal entities and individuals operating at different borders on a global scale. Culture, especially spiritual culture, is different for different peoples. But despite this, unfortunately, many researchers try to show that globalization also includes national cultures. For Example, S.Huntington connects civilization to language and religion, essentially ignoring the difference between culture and civilization [1]. Another American ideologist is Peter L. Berger takes the same position. It is no coincidence that under their joint edit, "multifaceted globalization" was published. The collective monograph" cultural diversity in the modern world " was written on the basis of this idea. Here, for example, an Indian version of cultural globalization, articles on cultural globalization in Hungary, Turkey and Chile are collected [2]. It turns out that each nation strives for globalization in its own way. In other words, this phenomenon was not a process that began in America and moved to the whole world, it includes the culture of all countries, and at this time each people themselves become a subject of globalization.

Journal Zone Publishing, Ilford, United Kingdom

In fact, the culture of different peoples can be equated in two extreme cases (polarization effect). When it falls to an extremely low level, to the level of instincts or to a very high peak of art, we can talk about rapprochement and spontaneity. Because when primitive feelings prevail, there will be no national culture at all, in which man acts not as a representative of the nation, but as a biological being. At this level, one can only talk about popular culture. On the other hand, when the scale and level of self-realization of a person as a social being is high, he strives for universal ideas. What he created is not only for one people, but for all mankind. And at this high point, national differences are eliminated. Thus, a person “deprives”a nation at both the lowest level and the highest level[3].

National culture is actually a transitional stage in a person's path from primitiveness to elevation, from animal instincts to divine feelings. In the cultural spectrum of most peoples, signs of both poles can be found. The center of gravity is located in the middle. But what does globalization promise us? Raising people from the level of national culture to a higher status, or removing the difference between them and lowering them to the level of popular culture – is this difference precisely at the level of national culture?

As McDonalds has been proposed instead of a national dish, attempts are being made to replace national literature and art with a mass culture based on the universality of animal instincts in relation to erotic feelings and fear, panic. And for this, all the capabilities of modern technology and communication systems are used [4].

Falling from nationality to publicity, the national recession does not occur at the initiative of the people. Of course, executive power is the representative of every people. But the authors of the idea come from somewhere in the West. On the other hand, Why does America or Western Europe need this process? See, A.Chumakov's book, which we mention, also seeks answers to these questions. The author approaches the issue not from the level of national cultures, but from the level of scientific and technological progress, global problems. A.N.Chumakov based on Clarke's argument that “the future should not be forgotten, it should be created”, history speaks of the great responsibility that human beings take as a subtext. But the creation of the future requires real strength. Although the source of this power is in nature, A.N.Chumakov tries to show that global revolutions began after a period of post-industrial society, scientific and technological progress, technical revolutions. He sees globalization as a natural-historical process [5].

Culture is also a special stage of the process. While everything created by man belongs to culture as an alternative to nature itself, civilization also becomes part of it. However, in this case, national cultures can only be understood within the framework of spiritual culture. Material culture is the same as civilization. At this point, the question arises: is the driving force of history more related to spiritual or material culture? It is difficult to give an exact answer to this question. So it turns out that scientific and technical progress alone is not enough.

On the other hand, for some researchers, talking about a single civilization, the only self-awareness process of humanity, seems controversial. For example, Shpengler does not

Journal Zone Publishing, Ilford, United Kingdom

accept humanity as a subject and believes that it is impossible to talk about its general purpose. However, A.N.Taking a different position, Chumakov divides global progress into 5 stages as a systematic process. From the second half of the 18th century to the 20th century

Until the 20s, we are talking about the geographical and economic integration of humanity and, finally, to a large extent, political integration. As a second stage, A.N.Chumakov shows the processes that took place in the 20-60s of the 20th century, the unification of society against nature and the economic, political and even environmental aspects of this union. A.N.Chumakov presents the later stages as stages of globalization's self-awareness. He refers to the last phase as the post-globalization phase. This is the stage of human activity as a single subject, which, as it has not yet been achieved, has a hypothetical nature. In general, A.N.Chumakov's book, which we are talking about, is devoted to the processes taking place on a global scale and is involved in research not only at recent times. Thus, in the work, the ideological source of modern processes is traced from more fundamental events that began thousands of years ago [6].

In the early 21st century, cybertahdid is a concept that emerged to achieve goals. First of all, having studied the emergence of the concept of cyberspace, we can better understand the goal and determine the optimal way to combat this threat. So, first of all, let's focus on why such concepts as cyberspace, cyberspace, cyberterrorism, cybercrime and how all the countries of the world are fighting this threat.

The new world order that emerged after the end of the Cold War, that is, the new strategy of the United States, aims to permanently control the world in different ways in the global space. The factor that created the conditions for this was the loss of interstate borders in the past, when everyone was in a relationship with each other. The emergence of the need to resolve relations between different civilizations led to this being overcome by the Union of all. The basis for this was the weakness of the political, economic and social foundations of the states that gained independence after the collapse of the USSR and the lack of clear priorities for future development.

In modern times, the ideology of humanism has also changed. In the beginning of 18th century, the general idea of politics for 200 years of the Enlightenment, the driving force was the belief that humanity would be saved through a just social structure. It took various forms, giving rise to various political movements, such as the ideas of socialism, communism, fascism or the "general Welfare Society", first in Bismarck-era Germany and later in England, the United States and other countries". Despite the differences between them, there was an opportunity to create a perfect society that united these currents. Representatives of the recorded flows believed that the emergence of a perfect society leads to the maturation of a separately acquired individual. By the early 20th century, these goals were considered easy to achieve. Many at the time thought that material wealth was to provide people with food and clothing. But gradually, he realized that life was more complicated. It is known that people's needs also increase as well-being increases.

The founders of the theory of post-industrial society are rightfully Z.Bjezinski, D.Bell and E. Toffler. These scientists were the first to directly connect a new type of society with the concepts of “information” and “Information Technology”.

Cyberattacks are one of the biggest problems of the information technology age in which we live, we will not be mistaken. Cybersecurity measures must be taken to protect systems, networks and software from digital attacks. In modern times, the number of cyber crimes is increasing. According to cybersecurity company Harbor Networks, the number of cybercriminals in 2019 is 60 times higher than in the last 11 years. This is a very serious number. It is for this reason that cyber security should be very important for states, companies and individuals. Such attacks are usually aimed at obtaining confidential information, modifying and destroying them, extorting money from users, or disrupting the normal activities of companies. “...although cybersecurity can be called a set of measures to combat cybercrime. The concept of cybercrime combines many types of crimes in the field of information and Communication Technology. These include terrorizing the Virtual network, preparing and distributing viruses and other malware, illegal information, mass distribution of electronic letters (spam), hacking attack, illegal access to websites, fraud, copyright infringement, theft of credit card numbers and bank details and various other offenses. In these cases, the perpetrators set themselves the goal of causing material and moral harm to the “objects”of their interest. And life itself shows that cybercrime and the circle of those who commit it are expanding from year to year” [8].

As a result of the development of Information Technology in the 60s of the 20th century, professional level computer specialists-hackers appeared who knew operating systems to the fullest extent, went to its depths, were comprehensively interested in computers, knew programming at the highest level. Today, hacking networks, which are widespread all over the world, carry out financial transactions, achieve access to personal data of citizens, keep the official figures of state bodies under pressure. Recently, information has been circulating that some states have access to the electoral system, there are attempts to create propaganda in this area, and thus the possibilities of manipulation expand. Hackers find system errors or system vulnerabilities in any system structure, they know the causes of these vulnerabilities. Unfortunately, a number of computer users suffer material and moral damage as a result of ignorance and carelessness. To avoid these damage, you need to know some basic topics and take some safety precautions. Effective cyber security measures are very difficult to implement today, because despite the fact that people today have more devices, cybercriminals are increasingly playing the role of “inventor”. In turn, a number of computer users suffer material and moral damage as a result of ignorance and carelessness. To avoid these damage, you need to know some basic topics and take some safety precautions.

Cybersecurity is the practice of protecting computers, servers, websites, mobile devices, electronic systems, networks and data from malicious attacks.

“The basic principles for ensuring cybersecurity include: legality;

priority of protecting the interests of the individual, society and the state in cyberspace;

the only approach to the regulation of the cybersecurity sector;

priority of the participation of domestic manufacturers in the creation of a cyber security system;

The openness of the Republic of Uzbekistan to international cooperation in ensuring cybersecurity" [7].

It is also known as information technology security or electronic information security. The term is used in a variety of contexts, from business to mobile phones and computers, and falls into several general categories:

Network security is the practice of protecting a computer network from targeted attackers and malware.

Application security focuses on protecting software and devices from threats. When an application is stolen, information designed to protect it can also be accessed. It starts at a successful security stage, even before the application or device is launched.

Information security protects the integrity and confidentiality of information both in storage and transmission.

Operational security covers processes and decisions related to data processing and protection. This includes the permissions that users give when accessing the network and procedures that determine how and where data can be stored or shared.

The training of end users is aimed at the most unpredictable factor of cybersecurity: people. Anyone who does not follow the safety rules well can accidentally infect a safe system with a virus. Teaching users how to disable suspicious email attachments, avoid entering unknown USB drivers, and various other important lessons is very important for the safety of any organization.

With the increasing number of cyberattacks every year, global cyberspace continues to develop rapidly. The Risk Based Security report found that 7.9 billion units were data breached in the first nine months of 2019. This is more than twice the number of attacks that occurred during the same period of 2018 (112%).

As cybersecurity continues to grow in scope, the International Information Corporation predicts that worldwide spending on cybersecurity solutions will reach $ 300 billion by 2024. Cybercriminals seek financial benefits and attract single participants or groups targeting systems to disrupt operations. "Cyberbullying is the process by which an intruder deliberately communicates material or spiritual to someone through the Internet. Today, the obvious manifestation of cyberbullying is the fact that it causes material and moral damage to the victim, having stolen the victim's Financial Information" [8].

Cyberattacks often involve collecting data for political reasons. Cyberterrorism is designed to disrupt electronic systems in a way that causes panic or fear. "Cyberterrorism is the use of computer and telecommunication technologies (mainly the Internet)in the path of terrorist goals. Cyberterrorism also provides for the seizure of computer control networks through special hacker programs and the occurrence of terrorist attacks on the Internet using computer viruses, the decommissioning of the

Internet network. The term was first used in the 1980s by Barry Colleen, a senior research fellow at the Institute for Security and Intelligence (US)" [8].

In our country, it is important to strengthen cyber security through artificial intelligence. In recent years, a number of cyber attacks have revealed the vulnerability of popular software and technology platforms. He argues for the need for strict cybersecurity laws. Leading global companies have strengthened the security of their systems to prevent cyberattacks. Artificial intelligence mechanisms are emerging to enhance cyber security and prevent attacks.

In addition to financial losses, cyber attacks also undermine the reputation of companies. This reveals serious security concerns regarding the company and its risk management practices. Cyberattacks prevention requires strategic planning and a qualified technical team. Over the years, we've seen data leaked from companies like Amazon and Facebook. Such incidents indicate the need for effective cybersecurity solutions.

"The development and support of the potential of personnel of Public Administration bodies, local government bodies and economic entities in the field of ensuring cybersecurity can be carried out through the following means:

providing financial, information and advisory assistance to organizations carrying out activities on retraining and improving personnel in the field of cyber security;

providing educational and methodological and scientific-pedagogical assistance in the field of ensuring cybersecurity.

Employees of important information infrastructure entities responsible for ensuring cybersecurity should improve their skills on a permanent basis in accordance with international standards and state standards and requirements" [7].

Artificial intelligence and "machine learning" are a new generation of technologies with intelligent applications. Artificial intelligence can transmit cyber security systems to protect against current and emerging threats. AI-enhanced solutions introduce advanced security mechanisms to protect against cyber attacks. The introduction of AI-based cyber security solutions can accelerate the growth of the data-driven security model.

Since the number of cyber attacks increases every year, the need to implement a security solution is very important and serious. With the advent of artificial intelligence, it is easier to create and manage a reliable and safe environment.

Let's see how artificial intelligence changes cybersecurity.

1) Use of biometric login:

Each person has a unique fingerprint, retinal (eye) impression. Using this biometric data to safely access the system can increase cybersecurity. Recently, many Amazon customers have experienced data corruption that put question marks on the Amazon security system. A statement released by Amazon through the Guardian explained the problem and explained it by technical error. Amazon insisted that the situation was under control and asked its buyers not to change their passwords. However, Richard Walters, the technical director of the cybersecurity firm CensorNet, disagreed. A large

Journal Zone Publishing, Ilford, United Kingdom

number of Amazon customers report having secret password security. Due to various breakdowns in the past, their passwords are available in dark hacks.

In addition to passwords, the use of biometric identifiers can increase the security of customer accounts with sensitive information. AI-based applications detect fingerprints, mesh curtains, and palm prints to deny access without authentication.

Currently, companies use 2-factor authentication to prevent data corruption. Since passwords are vulnerable to attacks, they can disrupt the user's personal information, credit card information, and Social Security numbers. Biometric identities prevent such attacks and provide secure access.

2) Detection of malware and threats:

Traditional cybersecurity techniques do not have the ability to detect and control malware. In 2018, estimates put the number of malware at 845 million. As of this year, 10 million malware attacks occur every month.

Requires a new generation of malware solutions. Therefore, cybersecurity firms are training artificial intelligence systems to detect next-generation threats. A report published in Forbes suggested that data security systems be trained with a “dataset” containing a variety of AI algorithms and other codes. Using such information, artificial intelligence can detect malfunctions in any application. Systems may take early steps to prevent a potential attack. In addition, artificial intelligence and “machine learning” play an important role in online security.

3) Prevention of conditional exit attacks:

Organizations use traditional authentication techniques to protect confidential information (information) from “uninvited guests”. But the use of the network may be at risk if an employee who has access to high authentication privileges remotely access the data. To prevent this, cyber security systems use artificial intelligence to create global identity systems. It should be noted that the artificial intelligence used in systems works in real time and is dynamic.

For this, artificial intelligence systems can use multi-purpose identification. Systems can also analyze the characteristics of people, networks, devices and places. After analysis, artificial intelligence automatically changes the user's access rights to protect data (data) on a remote network.

Since prevention is better than treatment, a robust defense system protects businesses from potential threats. Artificial intelligence systems give credibility to organizations fighting cyberattacks. As the types of attacks increase, artificial intelligence and “machine learning” create a security system to prevent malicious access. In cybersecurity solutions, many applications of artificial intelligence have taken on a new form. Large companies that have introduced artificial intelligence into their systems are fighting next-generation cyberattacks.

Cybersecurity has been declared one of the priorities of foreign policy in a number of countries (e.g. the United States, the European Union, Russia). The United States prepared a document in 2011 on the formation of the international framework of cyber security, which allows you to create a reliable, safe and open environment for free trade and socio-economic development. This document describes several basic principles. The first place is economic relations. The United States proposes to create free trade over the Internet by protecting private information, including trade secrets. Another important priority is the creation of an international code of ethics in cyberspace. According to the authors of the project, the presence of such code allows you to protect against foreign hacking attacks. Another paragraph is devoted to the fight against cybercrime. The U.S. calls on attention to focus on specific crimes and not restrict access to the internet. It is also envisaged to provide assistance to countries that do not have the opportunity to create a safe environment. The strategy covers all major U.S. ministries, all of which are tasked with creating principles of mutual cooperation with the participation of similar ministries in foreign countries.

What measures are being taken in this area in our country to protect against cybersecurity and risks? As in all countries, special attention is paid to cyber security at the state level in Uzbekistan. The state program, as well as the development concept of Uzbekistan-2035, continues to work on the solution of issues arising from the tasks set in the field of cybersecurity. In the mentioned documents, the training of private and other institutions in the field of cyber security and the formation of a culture of information security, the creation of appropriate technical and methodological tools in the direction of protecting information processes, strengthening cyber security, protecting information resources and systems from possible threats, increasing nationwide training in the field of cyber security, etc.k. such basic goals are set.

"State support for cyber security entities consists of:

improvement of the regulatory framework in the field of cyber security;

granting taxes, customs privileges and preferences to cybersecurity entities;

creating conditions for attracting funds of economic entities to finance the cybersecurity sector;

Organization of Public Procurement aimed at ensuring the guaranteed introduction of products and advanced technologies based on scientific and technological achievements in the field of cybersecurity;

assistance in training, retraining, as well as improving their skills in the field of cyber security" [7].

The Center for combating computer incidents operates as part of the Center for information security under the Ministry of development of Information Technologies and communications of the Republic of Uzbekistan. The main tasks and functions of the center include the collection, analysis and inclusion of relevant materials from users, computer equipment and software manufacturers and modern threats to computer security from similar structures in foreign countries, as well as information received about certain computer failures.

The main areas of activity of the electronic security service include coordinating the activities of information infrastructure entities in the field of cybersecurity, informing users about cyber attacks, illegal interventions, information systems and networks, malicious programs (electronic threats) aimed against the security of computer equipment.

To successfully ensure cyber security, it is necessary to organize several layers of protection covering protected computers, networks, applications or data. In the "online" world in which we live, advanced cybercrime programs serve for the benefit of each user. Cyber security includes key elements of critical infrastructure. This is of great importance for power plants, hospitals and financial services companies.

The strategy, which provides for the strategic planning and gradual implementation of activities in the field of information security and cybersecurity in the Republic of Uzbekistan, also sets out the following priorities:

Threat detection and risk management;

Strengthening measures and protection technologies for the detection of Information Security phenomena;

Increasing the level of information security of the information space;

Ensuring the safety of critical information infrastructures;

combating cybercrime, including strengthening activities in cybercriminology;

capacity building, institutional base development in the field of information security and cyber security;

Improving the regulatory framework of information security and cyber security;

Increase the culture of information security and cyber security;

Development of internal and international cooperation on information security and cyber security.

In addition, in accordance with the above-mentioned priorities, as well as the goals set and objectives to be achieved during the period provided for in the strategy, a plan of measures has been developed that include comprehensive measures in the field of information security and cyber security. We think that this plan, which includes multifaceted measures, will serve to successfully implement the strategy in general, by determining the main and other performers of approved measures for each measure, the duration of implementation and the indicators of the result.

REFERENCES:

1.Samyuel Xantington. Stolknoveniye sivilizatsiy. M. AST 2022. - 640s.;

2. Mnogolikaya globalizatsiya : kulturnoye raznoobraziye v sovrem. mire / pod red. Pitera L. Bergera i Semyuelya P. Xantigtona ; per. s angl. V. V. Sapova pod red. M. M. Lebedevoy. - Moskva : Aspekt Press, 2004. - 378 s.

3. Mironova L.V. GlobalizatsiY. Svetusheye mnogoobraziye natsiy [Tekst] / Larisa Mironova. - Beau Bassin, Mauritius : Lambert acad. publ., cop. 2017. - 156 s.;

4. Noskova YE.V. Adaptatsiya mejdunarodnix brendov tovarov i uslug k osobennostyam natsionalnix rinkov: teoriya i praktika. - Vladivostok : Morskoy gosudarstvenniy universitet imeni admirala G. I. Nevelskogo, 2020. - 149 s.

5. Chumakov A.N. Metafizika globalizatsii [Tekst] : kulturno-sivilizatsionniy kontekst : monografiya / A. N. Chumakov ; Rossiyskaya akad. nauk, In-t filosofii. - Izd. 2-ye, ispr. i dop. - Moskva : Prospekt, 2017. - 496 s.;
6. Chumakov A.N. Globalizatsiya : konturi selost. mira : monogr. / A. N. Chumakov. - Moskva : Prospekt : TK Velbi, 2005. - 428 s.; Chumakov A.N. Filosofskiye problemi globalizatsii [Tekst] : [monografiya] / A. N. Chumakov, A. D. Ioseliani. - Moskva : Universitetskaya kniga, 2015. - 171 s.; Chumakov A.N. Metafizika globalizatsii [Tekst] : kulturno-sivilizatsionniy kontekst : monografiya / A. N. Chumakov ; Rossiyskaya akad. nauk, In-t filosofii. - Izd. 2-ye, ispr. i dop. - Moskva : Prospekt, 2017. - 496 s.;
7. Qonunchilik ma'lumotlari milliy bazasi, 16.04.2022 y., 03/22/764/0313-son.

E-LEARNING RESOURCES:

8. https://ictnews.uz/uz/15/05/2018/cybercrime/;

Journal Zone Publishing, Ilford, United Kingdom