CONCEPTUAL ASPECTS OF RESEARCHING THE PROBLEM OF CYBER SECURITY

Uygun R. Turdiev

Independent Researcher National University Of Uzbekistan Named After Mirzo Ulugbek

Uzbekistan

ABSTRACT: This article analyzes the conceptual aspects of the study of cybersecurity problems. In particular, the content of the concept of cybersecurity, problems in this area, and the reasons for their occurrence are disclosed. Also, this article highlights the reforms in the Republic of Uzbekistan to ensure cybersecurity, regulatory frameworks, and participation in international rankings.

KEYWORDS: Cybersecurity, cyberspace, cyberculture, hybrid wars, threat, danger, phishing, software, international rating.

INTRODUCTION

Today, "in the political environment, not power, but the information factor has become more and more important. Foreign political success is determined not only by economic and military power but also by the success of democracy programs and mass democracy aimed at establishing control over the main informational and cultural processes in the world. Indeed, today, in a situation where information is becoming the "soft power" of every country, countries feel the need to create theoretical, practical, and conceptual foundations for ensuring their information security. Theoretically, the following situations can be components of the conceptual model of information security. These include threat objects, threats, sources of threats, targets of threats organized by the enemy, sources of information, obtaining confidential information (methods) through illegal means, directions of information protection, methods of information protection, and means of information protection. If we consider these as a conceptual model of information security in a general sense, each of these components is entering science as a paradigm in a new way and in a new form.

It is no exaggeration to say that cyber-attacks have united developed countries not only in relation to information but also geopolitically and geo-economically. We can say that the Russian cyberattacks in 2008, the hacking of Georgia's internet infrastructure in July of the same year, the attempt to hack the nuclear program of Iran by Israel and the US in 2012, or the attacks by Iran on the Pentagon .

We know that the 2020 internal information security market has grown by 25%. In other words, there are three reasons for this growth. First, there is a scientific need to study information security, and secondly, the development of cybercrime activity from year to year as a result of new threats and their increase in number based on the increasing relevance of information security. Accordingly, due to the strengthening of the COVID-19 pandemic in international relations today, states, companies and international TMCs in the cyber security market have increased their concern about conducting their cooperation and business based on individual risks. That is, due to the transition of business representatives and civil servants to the remote work system, and the freezing of money in banks, the development of cybercrimes has intensified due to the pandemic. There has been an increase in the number of attacks against the private parts of corporate services available around the world. As a result, attacks against vulnerabilities and flaws in the software of the public and private sectors led to an increase of up to 30% by 2020 (from 9% in the first quarter). This has spanned the range of cybercriminals from state actors to cyber espionage in corporate networks. This has led to the trend level of creating a safe environment in the cyber security market, as well as the need to create new problems and concepts in front of science.

Conceptual content of the concept of cyber security

"Cybersecurity", "cyberspace" in modern political-military sciences , "cyberculture" , "Proxy war", and "hybrid wars" categories entered. The increased demand for understanding these categories is related to the theoretical and practical needs of the state and society. Because the urgent need to make a decision on the issue of cyber security in a new environment requires a deeper study of these issues.

"Cybersecurity" as a category - is interpreted differently in sources. In particular, cyber security is an activity aimed at protecting information systems, networks, and programs from digital attacks. Typically, the goal of such attacks is to obtain, change or lose confidential information, extort money from users, or disrupt business processes. . In other words, cyber security means protection against accidental and deliberate information attacks. It is a multifaceted field of activity, and only a systematic and comprehensive approach to it can bring success.

Based on this, it can be said that the following types of cyber security threats can be included today:

Fishing - This is understood as sending fake e-mail messages that look like messages from the intended recipients. The purpose of this crime is to learn about the privacy of credit card numbers and credentials.

Virus extortionists or distributors - theft of funds by blocking access to computer systems during the payment process of the user.

Malicious software - is software designed to gain unauthorized access or damage to a computer.

Social engineers – attackers use social engineering to trick you into revealing sensitive information. They can commit crimes by asking you to transfer money or provide access to confidential information.

Web servers - we can see attacks made by extracting data and injecting bad codes in web applications. Cybercriminals distribute malicious code through the web servers they develop. We can also say the threats organized by code encryption, IPv6: the new internet protocol.

The term cyberspace is associated with the publication of Neuromancer, the first novel of a trilogy called "Cyberspace" by writer William Gibson in 1984. It describes the virtual space in which electronic data circulates on all computers in the world . Cyberspace is a field of communication carried out through computer networks, which has been developing and improving on a large scale since 1990. From a social point of view, when we say cyberspace, we mean a group of people or groups connected to each other through a computer network and entangled in the graphical information of any existing computer that intersects at different geographical points at the same time.

Today, as a result of the politicization of religion in political processes, threats under the guise of religion are increasing in cyberspace. On the websites of extremist organizations under the guise of religion, they mainly post information about religious leaders' calls for coup d'état and bloody wars. These messages and appeals are aimed at getting the young people to their hook by having a strong psychological impact on them. For example, extremist groups create fake profiles such as "Mustafa Mujakhid", "Abul Maviya", "Ansar-Ansar", and "Abu Ali" on social networks "Odnoklassniki", "Facebook", "Instagram", "Twitter", "Vkontakte". through the medium of propaganda, ideas, and appeals that promote subversive and alien ideas have a psychological effect on the minds of young people and invite them to go to the countries of the Middle East in order to "jihad".

Cyberculture - a technocratic new direction in the development of culture. It is a concept based on the possibilities of computer games and the use of virtual reality technologies . In today's global information space, this term is understood as a conscious restriction of the use of information that has a negative impact on the social consciousness, that is, destructive, unethical and biased information in the virtual network.

Proxy war -(Eng. proxy or proxy war) is considered to be the maintenance and extension of majorities between two countries in order to achieve their goals through military actions using resources as a result of the intervention of third-party donors.

Hybrid wars-"Soft power" is a means of influence using military force and means based on the policy. "Hybrid warfare" is the use of conventional, irregular, and asymmetric means combined with constant manipulation in political, ideological, and other spheres .

Regulatory and legal aspects of cyber security of Uzbekistan and participation in international ratings

In the Republic of Uzbekistan, 17 legal documents, 9 Presidential Decrees, and Decisions, 14 Cabinet Decisions, as well as relevant norms and many inter-departmental regulatory legal documents related to cyber security have been adopted.

In the Strategy of Actions on Five Priority Areas of the Development of the Republic of Uzbekistan, measures to protect the country's constitutional system, sovereignty, and territorial integrity within the framework of the fifth area called "Ensuring security, inter-ethnic harmony and religious tolerance, conducting a well-thought-out, mutually beneficial and practical foreign policy" implementation, improvement of the normative and legal framework of the field of cyber security was defined.

In particular, it was decided to develop a national cyber security strategy for 2020-2023, a draft law "On Cyber Security" and a unified information policy concept of the Republic of Uzbekistan. Decree of the President of the Republic of Uzbekistan dated November 21, 2018It is the Decision "On additional measures to control the introduction of information technologies and communications and improve their protection system". According to this Decision, the state unitary enterprise "Technical Assistance Center" was transformed into "Cybersecurity Center". It is precisely the purpose of the reorganization of this center that priority reforms aimed at creating a "safe information society" environment in our country have been set.

In addition, the normative and legal basis for Uzbekistan's participation in international ratings in recent years was determined. The purpose of this is to improve the position of the Republic of Uzbekistan in economic and political-legal international ratings and indexes, to effectively coordinate the activities of official ministries and agencies in this regard, to further raise the position of our country in the international arena, and to systematically reform cooperation with foreign rating agencies. In particular, the President of the Republic of Uzbekistan March 7, 2019"On Systematization of Measures to Improve the Position of the Republic of Uzbekistan in International Ratings and Indexes" No. PF-5687and decrees No. PF-6003 dated June 2, 2020 "On improving the position of the Republic of Uzbekistan in international ratings and indexes and introducing a new mechanism of systematic work with them in state bodies and organizations" .

In this way, the most important indicators of efficiency (hereinafter - KPI) according to the international rating and indices, which are priority for the Republic of Uzbekistan, have been approved. In order to systematically analyze these indicators, the Republican Council for Working with International Ratings and Indexes was established. The main task of this council is to:

- to carry out a systematic analysis of the country's level of socio-economic and political-legal development, to ensure that fundamental changes implemented in various fields serve the goals of improving the country's position in international ratings and indexes that are a priority for the Republic of Uzbekistan, and to eliminate problems that hinder the effectiveness of work in this direction;
- In order to improve the country's position in the international rankings and indexes, which are a priority for the Republic of Uzbekistan, to advance initiatives to improve the system of state power and management, democratize society, implement reforms in the field of state and society building based on advanced international experience;
- a comprehensive evaluation of normative legal documents aimed at regulating various aspects of state and community life and their projects in terms of impact on the country's place in international rankings and indexes, which are priority for the Republic of Uzbekistan. This Council conducts its activities in the field of socio-economic and political-legal rating and indices, divided into working groups in the field of national rating and indices. It is in the E-Government Development Index (E-Government Development Index) that Uzbekistan is undergoing reforms to improve its position in international rankings and indexes.

No	Naming categories	Current status	2020 year	2022 year	2030 year
1	E-Government Development Rating (E-Government Survey)	0.62 (81st place)	0.66	0.70	0.86

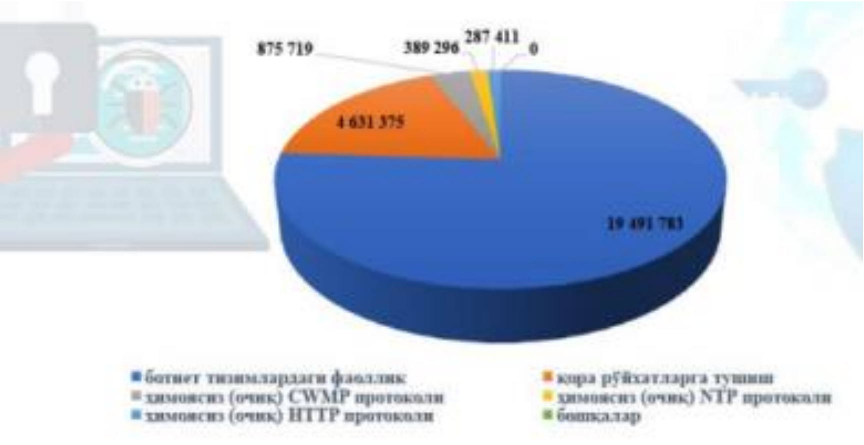
We can see from this index that the development of the infrastructure of information and communication technologies in our country, by ensuring cyber security, is to improve its position in international rankings. For this purpose, in order to increase the prestige of our country in the international community and to ensure the execution of assigned tasks, the Ministry is conducting cooperation with relevant ministries, departments and research institutes for each index.

"Digital Uzbekistan - 2030" strategy by the Decree of the President of the Republic of Uzbekistan dated October 5, 2020 confirmed. In this strategy, the active development of the digital economy in our country, the widespread introduction of modern information and communication technologies in all sectors and fields, first of all, in public administration, education, health care and agriculture. In particular, in the strategy, the target indicators of the "Digital Uzbekistan - 2030" strategy, the transformation program, the coordination commission for implementation, the "Roadmap" for the implementation of the connection of networks and regions to the diplomatic missions of the Republic of Uzbekistan in foreign countries have been developed. In general, these normative legal documents are measures aimed at increasing the international image of Uzbekistan based on the development of digital technologies.

However, along with the progress being made, there are also gaps in the field of cyber security. We looked at cyber security as internal and external challenges in our research;

Internal problems.

According to the 2020 report of the Cyber Security Center of the Republic of Uzbekistan, over 27,000,000 malicious and suspicious network incidents threatening information and cyber security were observed in the national Internet segment in 2020 (Figure 1). Among them:



(1 – Расм: Кузатилган таҳдидларнинг асосий салмоғи)

It was found that most of the above-mentioned threats are in the address group of Uzbektelecom, Uceel, and Beeline companies. In 2020, during the implementation of measures to increase the security of modern information systems and resources of the national "UZ" domain, 297 studies and examinations were conducted. As a result of the work carried out, 695 vulnerabilities were identified, and information systems and resource owners were immediately notified. Majority of identified vulnerabilities

- 466 of extremely dangerous level;
- Medium dangerous level - 205;
- 24 of low risk level.

The above-mentioned vulnerabilities were eliminated in time and the theft of confidential information of citizens of the Republic of Uzbekistan was prevented. .

External problems

We looked at it from the point of view of the participation of the reforms of the Republic of Uzbekistan in the field of cyber security in international ratings. Because, although large-scale effective work is being carried out in the field, the results of analyzes and evaluations of ratings by international organizations show that ensuring cyber security is of urgent importance in our country. In particular, the International Telecommunication Union (ITU) of the UN is an international institutional organization that ensures cooperation of the countries of the world in the field of information and communication. This institutional organization is recognized as an ancient organization founded on May 17, 1865 as the International Telegraph Union. . This organization was established on November 15, 1947 based on the agreement on a specialized agency in the UN system, and officially became an international organization that came into force on January 1, 1949, and 193 countries are members. . The independent Republic of Uzbekistan is also a member. One of the main tasks of this organization is the development of satellite orbits, the development and development of world technical standards, and cooperation in the improvement of wireless technologies around the world.

This international organization annually publishes "Information Society Indicators" and "Kon e-security" publishes annual global rating reports. For example, if we pay attention to the reports published by the International Telecommunication Union (ITU), in 2017, Uzbekistan took 93rd place in the global ranking of cyber security. In that year, Uzbekistan scored 0.277 points in the new rating and shared the 93rd place with Jordan. We can see that Uzbekistan ranks 9th among the CIS countries .

The international global rating on cyber security is a joint project of ABI Research and the International Monetary Fund, and the index allows to assess the level of participation of countries in the field of cyber security. The level of commitment is assessed in five areas: legal measures, technical measures, organizational measures, capacity development and international cooperation. According to the 2020 summary of global cyber security rankings, Uzbekistan ranks

90th in the National Cyber Security Index, 52nd in the Global Cybersecurity Index, and 95th in the ICT Development Index. we can see that

Also, the British research company Comparitech publishes a ranking of countries with a relatively high level of cyber security. 60 countries are included in this ranking, and Japan is leading it. The last place was occupied by Algeria. Uzbekistan was also included in the list, and it took the 56th place. This rating7 criteria, including the share of mobile devices and computers infected with malicious software, the number of hacking attacks carried out for the purpose of stealing money, the preparedness of this or that country for hacking attacks, the presence of relevant legislation, etc. Each country can score from 0 to 100, with the lower the score, the better the country is protected from cyber threats. According to the final table, Japan scored 8.8 points. France and Italy took the 2nd and 3rd places. These countries scored 10.6 and 11.2 points, respectively. The top ten countries are Denmark, USA, Ireland, Sweden, Great Britain, Netherlands and Singapore. Algeria, which took the last place in the rating, scored 55.8 points. Uzbekistan ranked 56th with 50.5 points. It should be noted that Uzbekistan was the only Central Asian country included in the rating. .

Proposal and conclusion

These analyses once again confirm the relevance of the issue of cyber security, because software vulnerabilities can cause an attacker to remotely access an information system or website, as well as files and data, and leak the personal data of citizens. Cybersecurity measures prevent such situations.

In order to protect citizens from cyber attacks, it is necessary to use protective codes (passwords) in mass media, information distribution devices, and electronic money transfer processes. This code must be kept secret, and the antivirus programs on the devices must be constantly activated.

Uzbekistan is gradually transitioning to a digital economy. In this environment, security and stability in data storage, transmission, and processing is an important factor. In this regard, responsibility and attention are required, especially from the employees of state bodies. It is necessary to organize seminars on the topic of cyber security among the population, youth, and communities. Such measures help to eliminate the regular small attacks of software hackers (hackers).

In general, the systematic and fundamental approach to ensuring cyber security in Uzbekistan, the creation of a unified regulatory legal document base, the introduction of advanced foreign experience, and the wide use of innovative methods contribute to the effective implementation of the state information policy and the solution of problems in the field of information security.

This is determined by protecting the information communication and technology system from modern cyber threats, introducing modern cyber security mechanisms for different levels of systems, defining the rights and obligations of state bodies, enterprises and organizations in this field, and coordinating their activities. It is possible to improve the provision of cyber security through the unification of regulatory legal documents in this area.

At the heart of all the reforms being carried out in our country is the goal of creating comfort for our people. A special focus on cyber security is the basis for using digital opportunities in a reliable and secure way.

REFERENCES

1. Blackwill R, Harris DJ. "Voyna inymi sredstami" Geoeconomika i iskusstvo upravleniya gosudarstvom.Izdanie na russkom yazyke AST Publishers, 2017. – S. 105.
2. Cyber Security 2020–2021.https://www.ptsecurity.com/
3. This concept is related to the publication of the first novel of the trilogy called "Cyberspace" by the writer William Gibson "Neuromancer" in 1984. It describes the virtual space in which electronic data circulates on all computers in the world. See: Annotated Dictionary of Information Communication Technologies. UNDP representative office in Uzbekistan. - 2010. - 573 p.
4. A technocratic new direction in the development of culture. It is based on the possibilities of computer games and the use of virtual reality technologies. That source.
5. https://www.cisco.com/c/ru_ru/products/security/what-is-cybersecurity.html
6. See: Annotated Dictionary of Information Communication Technologies. UNDP representative office in Uzbekistan. - 2010. - 573 p.
7. See: Annotated Dictionary of Information Communication Technologies. UNDP representative office in Uzbekistan. - 2010. - 573 p.
8. See:https://regnum.ru/news/polit/2421809.html
9. Decree of the President of the Republic of Uzbekistan No. PF-5687 of March 7, 2019 "On Systematization of Measures to Improve the Position of the Republic of Uzbekistan in International Ratings and Indices"/https://lex.uz/docs/4230916
10. Decree No. PF-6003 of the President of the Republic of Uzbekistan dated June 2, 2020 "On improving the position of the Republic of Uzbekistan in international ratings and indexes and introducing a new mechanism of systematic work with them in state bodies and organizations"/https://lex.uz/docs/4838762
11. Famoni of the President of the Republic of Uzbekistan dated October 5, 2020 on the "Digital Uzbekistan - 2030" strategy" and measures for its effective implementation".https://lex.uz/docs/5030957
12. 2020 report of the Cyber Security Center of the Republic of Uzbekistan.https://tace.uz/uz/
13. https://en.wikipedia.org/wiki/International_Telecommunication_Union
14. "The oldest organization of the UN system, the International Telecommunication Union celebrates 150th anniversary | MPO". mpo.cz. Retrieved 27 August 2020
15. https://kun.uz/52930503
16. https://www.itu.int/ru/Pages/default.aspxhttps://www.abiresearch.com/https://hordiq.net/2020/12/07/uzbekistonda-kiberhafsizlizni-tasetsen-davr-talabi-anahlil-va-tavsiyar/
17. https://kun.uz/news/2019/02/07/cyberkhavfsizlik-darajasi-byyache-eng-yaksh-davatlar-retingi-tuzildi-uzbekiston-ohirgi-beshtalikda