The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
VOLUME 05 ISSUE 04 PAGES: 01-04
SJIF IMPACT FACTOR (2020: 5. 453) (2021: 5. 952) (2022: 6. 215) (2023: 7. 304)
OCLC – 1176274523
Publisher: The USA Journals

Journal Website: https://theamericanjournals.com/index.php/tajpslc

Research Article

THE ROLE AND IMPORTANCE OF STATE MANAGEMENT IN THE FIELD OF CYBER SECURITY IN UZBEKISTAN IN THE CONTEXT OF GLOBAL CHANGES

Submission Date: April 02, 2023, **Accepted Date:** April 06, 2023,
Published Date: April 12, 2023 |
Crossref doi: https://doi.org/10.37547/tajpslc/Volume05Issue04-01

Uygun R. Turdiyev
Researcher Of The National University Of Uzbekistan

ABSTRACT

This article reveals the role of cyber security in the process of globalization and its negative consequences. Also, the reforms carried out in the Republic of Uzbekistan to ensure cyber security and their practical importance are analyzed.

KEYWORDS

Cyber, cybercrime, cyber security, cyber extremism, cyber security architecture, global space, government.

INTRODUCTION

In today's global information space, security is of fundamental importance. International cyber security architecture shows that it is necessary not only to meet modern requirements, but also to take into account the prospects of technological development. These scientific advances indicate that another global problem should be put on the agenda. This has led to the emergence of a new type of crime related to the distribution of various viruses, password cracking, illegal information distribution, hacking attacks, illegal access to websites, fraud, copyright infringement, and credit card theft. According to data, cyberattacks cost the world economy an average of $26 billion a year [1]. For example, more than 500 million cyber-attacks are organized around the world every year. Every second, one in 12 people become victims of cyber attacks. In

The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
VOLUME 05 ISSUE 04 PAGES: 01-04
SJIF IMPACT FACTOR (2020: 5. 453) (2021: 5. 952) (2022: 6. 215) (2023: 7. 304)
OCLC – 1176274523
Publisher: The USA Journals

developed countries such as the United States of America, France, England, Germany, Belgium, Luxembourg, 60-65 percent of crimes are committed through cyber attacks [2]. Experts say that the increase in the number and scope of cyber threats is mainly caused by the fact that state bodies and organizations use devices that do not meet the established security requirements. In addition, the fact that the legislative documents on the prevention of cyber threats are not perfect, that the legal basis for mutual cooperation between the authorized state body, communication operators and network owners is not provided, and that a single body that ensures information and cyber security has not been established has become a global problem. Even in the Central Asian region, the issue of cyber security is gaining importance. The President of the Republic of Turkmenistan, Serdar Berdimuhamedov, also acknowledges this. That is, "modern challenges and threats to the Central Asian region, including the fact that one of the main problems in the world is the security sector, "illegally creating foreign ideas from information technology and the attitude against the historical traditions, main values and centuries-old principles of life of the Central Asian peoples" emphasizes [3]. In his speech, the President of Turkmenistan, Serdar Berdimuhamedov, emphasized the need to work together to fight the illegal use of information technologies and to establish a comprehensive security system for five countries in order to continue the development of Central Asia in an environment of stability and prosperity. For example, among the most attacked industries in the world in 2021, the first place was taken by the education and research sector - 1605 (a 75% increase in attacks compared to 2020). 1136 attacks were carried out on state and defense organizations (+47%); communication – 1079 (+51%); health care - 830 (+71%) how important it is to ensure cyber security.

THE MAIN FINDINGS AND RESULTS

The increase of problems and risks in cyberspace in our country, the sharp increase in cybercrime, the increase in online attacks and the unpredictable dynamics of the development of cyberspace in the world have shown the need to develop a regulatory and legal framework for ensuring cyber security in the Republic of Uzbekistan and define the functional obligations of state administration bodies in this regard. The reason is that, according to the data of the state unitary enterprise "Cybersecurity Center", during 2020, more than 27,000,000 malicious and suspicious network incidents threatening information and cyber security were observed in the national Internet segment. Also, 680 incidents occurred within the framework of ensuring the security of information systems and websites, including when websites were down for 1,000,000 minutes due to malfunctions [4], In 2021, more than 17,097,478 malicious and suspicious network incidents threatening information and cyber security were observed in the national internet segment. In addition, 636 incidents occurred within the framework of ensuring the security of information systems and websites, in particular, failures caused the failure of websites for 1,048,216 minutes [5].

In particular: by the decision of the Cabinet of Ministers of the Republic of Uzbekistan No. 555 of November 24, 2004 "On measures to improve the management structure in the field of mass communications", the state institution "Monitoring Center in the field of mass communications" was established. According to this decision, the main tasks of the Center are to carry out systematic monitoring of the activities of the national information space and mass communication media, including modern information and communication technologies, satellite systems, the global network of the Internet, other electronic means

The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
VOLUME 05 ISSUE 04 PAGES: 01-04
SJIF IMPACT FACTOR (2020: 5. 453) (2021: 5. 952) (2022: 6. 215) (2023: 7. 304)
OCLC – 1176274523
Publisher: The USA Journals

of information transmission and distribution, as well as printing products, and the introduction of new technologies. improvement of the monitoring system in the field of mass communications, formation of information resources, information transmission and distribution systems and tools, and other similar tasks were envisaged. The Ministry of Information Technologies and Communications Development of the Republic of Uzbekistan was established by the Decree of the President of the Republic of Uzbekistan No. PF-4702 dated February 4, 2015 "On the establishment of the Ministry of Information Technologies and Communications Development of the Republic of Uzbekistan". It was designated as an authorized body in the field of communication, information and telecommunication technologies. In the Decree of the President of the Republic of Uzbekistan dated February 19, 2018 "On measures to further improve the field of information technologies and communications", implementation of comprehensive measures to ensure cyber security and ensure the introduction of networks, software products, information systems and resources, collection of personal and biometric data, special attention is paid to the issues of participation in the regulation of the use of processing and storage technologies. On September 14, 2019, the decision of the President of the Republic of Uzbekistan No. PD-4452 "On additional measures to control the introduction of information technologies and communications and improve their protection system" was adopted. Based on this decision, the state unitary enterprise "Technical Assistance Center" of the Cabinet of Ministers, the State Security Service and the Ministry of Information Technologies and Communications Development was transferred to the State Security Service and renamed as the "Cybersecurity Center" state unitary enterprise. Also, in order to regulate relations in the field of protection of children from information harmful to their health, the Law of the Republic of Uzbekistan "On protection of children from information harmful to their health" was adopted. By law, the Information and Mass Communications Agency under the Administration of the President of the Republic of Uzbekistan was designated as a specially authorized state body in the field of protecting children from information harmful to their health.

In this Law, the specially authorized state body must implement the unified state policy in the field of protecting children from information harmful to their health, participate in the development and implementation of state programs and other programs in the field of protecting children from information harmful to their health, protect children from information harmful to their health. it is envisaged that the information provider will exercise control over the implementation of the legislation on protection of information and other similar tasks. In turn, on April 15, 2022, the Law of the Republic of Uzbekistan "On Cyber Security" No. O'RQ-764 was adopted in order to continue reforms in this field, including regulating relations in the field of cyber security [6]. This law consists of 40 articles. In accordance with this Law, protection of the interests of individuals, society and the state from external and internal threats in cyberspace was noted as a priority in ensuring the cyber security of the state. The law defines the main concepts in the field of cybercrime, cyberspace, cyber threat, cyber security, cyber protection, cyber attack.

The following aspects of cyber security are legal in this law; the priority of protecting the interests of the individual, society and the state in cyberspace; unified approach to cyber security regulation; the priority of the participation of local manufacturers in the creation of a cyber security system is established. In addition,

The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
VOLUME 05 ISSUE 04 PAGES: 01-04
SJIF IMPACT FACTOR (2020: 5. 453) (2021: 5. 952) (2022: 6. 215) (2023: 7. 304)
OCLC – 1176274523
Publisher: The USA Journals

the main principles of the Republic of Uzbekistan, such as openness to international cooperation in ensuring cyber security, have been defined. It was envisaged that the President of the Republic of Uzbekistan will determine the unified state policy in the field of cyber security. In turn, the State Security Service of the Republic of Uzbekistan was designated as the competent state body in the field of cyber security. It is envisaged that the examination of compliance with cyber security requirements shall be carried out in a mandatory manner or at the initiative of cyber security entities, and the following shall be subject to the examination of compliance with cyber security requirements in a mandatory manner: - information resources of state bodies; - information systems of state bodies; - information systems included in the category of important information infrastructure objects.

It was determined that the hardware, software, hardware and software tools used in order to ensure the cyber security of the information systems and resources of state bodies and organizations, as well as important information infrastructure objects, must be certified in a mandatory manner. Also, according to the Law, taking measures against cyber security incidents by cyber security entities can be carried out in the following forms: elimination of vulnerabilities and errors in software and devices;

destroy malicious programs, limit their spread, technically limit the source of cyber attacks;

isolation of information objects from existing cyber threats;

providing information about cyber security incidents to law enforcement agencies.

CONCLUSION

In conclusion, it should be noted that this Law is important in ensuring cyber security of the state as a legal mechanism for protecting the interests of individuals, society and the state from external and internal threats in cyberspace. In addition, the state policy in the field of ensuring cyber security in our country is aimed at regulating social relations in the field of cyber security, which determines the main tasks and directions of activities of state authorities and administrative bodies, as well as the role and importance of citizens' self-government bodies, public associations and other non-governmental non-profit organizations, citizens serves.

REFERENCES

1. http://hudud24.uz/kiberhavfsizlik-zamon-talabivaziyat-ta%d2%9bozosi/.
2. https://iiv.uz/oz/news/kiber-makonda-sodiretilayotgan-jinoyatlarga-qarshi-kurashish-muammolar-va-yechimlar.
3. https://turkmenistan.gov.tm/ru/post/68980/informacionnaya-bezopasnost-prioritetnaya-zadacha-centralnoaziatskogo-regiona
4. Final reports of 2020-2021 prepared by the state unitary enterprise "Cybersecurity Center". https://tace.uz/upload/iblock/9d5/1.%20%D0%98%D1%82%D0%BE%D0 %B3%D0%B8%202021_%D1%83%D0%B7.pdf
5. Decision No. 555 of the Cabinet of Ministers of the Republic of Uzbekistan dated November 24, 2004 "On measures to improve the management structure in the field of mass communications".
6. Law of the Republic of Uzbekistan "On Cyber Security" adopted on April 15, 2022 ORQ-764.// https://lex.uz/uz/docs/5960604