CHARACTERISTICS OF THE CENTRAL ASIAN CYBERSECURITY SYSTEM

Mokhigul Rahmanovna Mayusupova [1]
[1] *Tashkent State University of Oriental Studies*
2nd year master's student, International Relations and World Politics
e-mail: mohigulmayusupova@gmail.com

MAQOLA MALUMOTI

MAQOLA TARIXI:
Received:09.01.2025
Revised: 10.01.2025
Accepted:11.01.2025

KALIT SO'ZLAR:
Cybersecurity, Central Asia, digital infrastructure, regional cooperation, government policy, security issues, international cooperation.

ANNOTATSIYA:

As cyber threats become more sophisticated, we can see an increase in the number of cyber attacks targeting the government, financial and industrial sectors. This article examines the specific features of cyber security systems in the Central Asian region, and gives a detailed opinion about the existing problems and opportunities in the region. Also, the measures taken by the countries located in the Central Asian region to strengthen cyber security measures were analyzed and the current state of cyber security was given based on percentages. In addition, in the article, the author highlighted the common and different aspects of cyber security approaches in the republics located in the Central Asian region, including: Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan and Uzbekistan.

INTRODUCTION. The development of regional security issues in Central Asia. Regional political processes and regional security issues emerged as a new scientific research object in the early 20th century within the framework of such disciplines as political science and regional studies. In particular, regional security problems in the Central Asian subregion, like those in the rest of the world, are represented by terrorism, extremism, the spread of weapons of mass destruction, the increased threat of nuclear weapons, drug trafficking, environmental degradation, global warming, deforestation, the spread of pandemic diseases and other threats. The risk of wars related to the distribution of water resources is also growing. In addition, the countries of this region have not yet been able to find adequate answers to many old and new problems of an internal, endogenous nature. In recent years, it can be seen that the digital landscape of Central Asia has undergone rapid changes, which in turn has led to increased attention to cybersecurity.

In particular, the main cybersecurity threats in Central Asia include:

Cybercrime: The region faces threats from cybercriminal groups engaged in financial fraud, data theft, and other illicit activities. The economically strong Kazakhstan and Uzbekistan are the main targets.

Cyberterrorism: Given the political instability in some parts of the region, the threat of cyberterrorism, in which extremist groups use cyberspace to spread propaganda and destabilize, has been identified as a growing concern.

Data privacy and protection: Enforcement of data protection laws is patchy across the region, with countries like Kazakhstan making progress in this area, while others like Turkmenistan have not adopted comprehensive data protection regulations.

METHODS

A mixed and comparative analysis method combining qualitative and quantitative research was used to study cybersecurity systems in Central Asia.

RESULTS

The cybersecurity landscape of Central Asia is characterized by varying levels of technological development and status. Countries such as Kazakhstan and Uzbekistan have made significant progress in creating robust cybersecurity infrastructures, while countries such as Turkmenistan and Tajikistan lag behind in terms of investment and development.

After gaining independence in 1991, Uzbekistan, Kyrgyzstan, Tajikistan, Kazakhstan, and Turkmenistan faced a completely new threat to national security. In the past decade, the number of existing problems has increased due to the emergence of high-tech and Internet-based crimes. Cybersecurity is closely related to the spread of the Internet and is observed in all Central Asian countries, despite changes in network connection speeds. According to Ookla, which has been testing internet speeds every 30 days since February 2014, Kazakhstan ranked 58th, Tajikistan 66th, Kyrgyzstan 81st, and Uzbekistan 171st out of 188 countries. According to the same source, Kazakhstan ranked 38th out of 192 in the 2020 Global Cybersecurity Index compiled by experts from the United Nations International Telecommunication Union. Uzbekistan ranked 78th, Kyrgyzstan 100th, and Tajikistan 146th. Cybercrime in Central Asia falls into three main categories: hooliganism, hacking, and computer fraud. According to the results of the United Nations survey in 2018, 50% of countries do not have a cybersecurity strategy, while 25% of countries have a legal framework for the security of critical information infrastructure (CII). It was also found that only 31% of countries include a section on the protection of CII in their cybersecurity strategy, and only 109 participating countries have cybersecurity legislation. 141 countries (73%) have online privacy laws.

Based on this, we analyze the cybersecurity system and its specific features in the Central Asian region as follows;

The Republic of Kazakhstan is a country with a place in Central Asia. Democratic changes began in its political system after 1991. The adoption of a six-year National Program (2006-2011), designed for two stages, in this regard indicates a strong commitment to these reforms. However, the fact that the achievements of information and communication technologies are rooted in the formation of a culture of their use and in the social and production relations inherent in the “information society”, primarily in ensuring cybersecurity, is also characteristic of recent decades in Kazakhstan. In particular, Kazakhstan rose 9 places in the United Nations Global Cybersecurity Index, taking 31st place (previously 40th place). This was announced in the report of the 4th edition of the Global Cybersecurity Index at the conference of the International Telecommunication Union held on June 29. The rating is based on the state's legislative framework, technical and organizational measures, activities in the international arena and the potential for developing information security. Perhaps that is why the “Cybersecurity Concept” was adopted by the Resolution of the Republic of Kazakhstan in 2017. Cybersecurity Concept (“Cyber Shield of Kazakhstan”) (hereinafter referred to as the Concept). In accordance with the Address of the President of the Republic of Kazakhstan “The Third Modernization of Kazakhstan: Global Competitiveness”, the “Kazakhstan-2050” Strategy was developed taking into account Kazakhstan's approaches to entering the 30th place among the most developed countries in the world, (Кульжанова Г, 2005).

Until 2019, Kyrgyzstan did not have a state program to combat cybercrime. The Cybersecurity Strategy of the Kyrgyz Republic was developed and approved only in 2019, within the framework of which it is planned to create the basic conditions for ensuring cybersecurity in the country in 2019-2023. In addition, the strategy plans to introduce liability for cybercrimes, including cross-border computer crimes, into legislation, and introduce methods for identifying, collecting and presenting evidence using ICT. Issues of ensuring the digital protection of the Kyrgyz Republic have become the subject of political and academic discussions in recent years. It is known that the Global Cybersecurity Index of the International Telecommunication Union of the United Nations (UN) is a research project that serves the purposes of identifying the risks of obstacles to the development of the digital environment in the world, developing recommendations, strengthening the cyber defense of countries and forming a global digital culture. Kyrgyzstan has a relatively low score on this index. Since 2014, Kyrgyzstan has been included in the group of countries with a low level of cybersecurity. In 2017, it was in 96th place in the rating, but by 2018 it had fallen to 111th place and continues to lose its position. In the regional distribution of the index, Kyrgyzstan ranks 4th in Central Asia and 8th in the CIS, below it only Turkmenistan. Kazakhstan remains the leader in the Central Asian region; in the short period from 2017 to 2018, it rose from 82nd to 40th place in the world ranking, and from 7th to 2nd place in the CIS countries index, (Boʻtayev U.X., Turdiyev U.R., 2024).

According to the study, Tajikistan is the least protected country in the world in terms of cybersecurity, followed by Bangladesh and China. Tajikistan had the worst performance in terms of users attacked by banking malware (4.7 percent), computers attacked by at least one local malware attack (41.16 percent), and cryptomining attacks (5.7 percent). It also performed poorly in terms of users attacked by ransomware (1.35 percent). At the same time, it was one of the best performing countries in several metrics, including users attacked by web resources by country of origin (0.03 percent), Telnet attacks (0.01 percent), spam messages (0.01 percent), and the percentage of countries covered by malicious emails (0.01 percent). No user was attacked by mobile ransomware-trojans, and none of the SSH-based attacks originated from Tajikistan.

On November 7, 2003, the Republic of Tajikistan was the first among the countries of the region to adopt the Concept of Information Security. It is this concept that reflects specific goals in the information sphere in the country. The situations and directions of ensuring information security reflect the strategic goals of the state in the field of domestic and foreign policy, (Я.Ибодов, 2015).

With the expansion of the digital world, a new direction has emerged in the field of security, studying cybersecurity issues. Cybersecurity is based on knowledge based on ethical standards and technical infrastructures, interpreted by various international institutions or neutrally accepted. Cybersecurity has quickly transformed from a technical discipline into a strategic program. However, theoretical development is still at an early stage. Only by 2013 was a preliminary document adopted in this regard. On May 4, 2013, the Law “On National Security of Turkmenistan” was adopted. It is this document that considers the information space as a territory and defines the tasks of protecting it, activities related to its formation, creation, transformation, processing, transmission, use, storage, information affecting the information infrastructure, including its impact on individual and social consciousness. The reason for this procedure is that, according to the Law "On State Secrets" adopted in 1995, the issue of information transmission and exit in the country was strictly prohibited as censorship. That is, all channels transmitting information were controlled.

The Law of the Republic of Turkmenistan "On Mass Media", adopted on December 22, 2012, determined the sources of information dissemination. After that, the process of liberalization began in the reforms in this area. After the adoption of a new constitution in the political life of the country on September 14, 2016, it was established that "Everyone has the right to freely receive and seek information, and to disseminate information in a manner not prohibited by law, with the exception of those protected by state or other law." Thus, the country began to open up in the regional and global information space. On September 6, 2019, the President of Turkmenistan signed the Law "On Cybersecurity" and on September 9 of the same year established the Cybersecurity Service. At the same time, the State Program for Ensuring Cybersecurity in Turkmenistan for 2022-2025 was approved (Law of Turkmenistan "On Legal Regulation of the Development of the Internet Network and the Provision of Internet Services in Turkmenistan" dated December 20, 2014).

In the Republic of Uzbekistan, the Law "On Personal Data" was also adopted in 2019. It defines the structure, content of personal data, how and where they are stored. In addition, in 2022, the Law of the Republic of Uzbekistan "On Cybersecurity" was adopted. According to the law, protecting the interests of individuals, society and the state in cyberspace from external and internal threats is a priority in ensuring the state's cybersecurity. One of the indicators that reflects the ability to combat cyberattacks is the level of cybersecurity, and in this regard, the "Global Cybersecurity Index 2020" (GGI) report of some CIS member states is noteworthy. In particular, the transition of many sectors of activity and socio-economic services to digital format in the former Soviet Union countries, despite the problems associated with the pandemic, is evidence that these countries are working to improve their cybersecurity, (Bo'tayev U.X., Turdiyev U.R, 2024).

In general, despite the fact that regulatory documents against cyberattacks are being developed in cooperation with the Central Asian countries, the fact that cyberattacks still continue to occur remains the most sensitive aspect of the issue. In particular, as a result of the work carried out in this regard by the neighboring countries of our republic, the republics of Kazakhstan and Kyrgyzstan, despite the increase in malicious cyber incidents, have moved up the GCI list. In particular, although the number of Internet crimes in Kazakhstan increased by 139 percent, it took 31st place, bypassing China (33rd place) and Israel (36th place), and 2nd place among the CIS countries. The Kyrgyz Republic has eliminated 676,918 pieces of malware since 2019, moving up from 111th to 92nd place on the GCI list. Tajikistan ranks 138th on the list. It is ahead of its closest CIS neighbor Turkmenistan (144th), but is behind Kazakhstan and Uzbekistan in the Central Asian region.

DISCUSSION

The geopolitical environment in Central Asia has a significant impact on cybersecurity strategies. The region's political history, characterized by Soviet rule and subsequent post-Soviet transitions, has shaped the national security systems of Central Asian states. National governments, particularly in countries such as Turkmenistan and Uzbekistan, often view cyberspace as an extension of their political control.

State control over the Internet: Internet censorship is particularly prevalent in countries like Turkmenistan, where the government controls almost all access to the Internet. This centralized control creates a paradox that, while limiting certain cyber threats, it also hinders the development of a competitive cybersecurity landscape with neighboring countries.

Influence of Russia and China: Both Russia and China have an impact on cybersecurity policy in Central Asia. For example, Kazakhstan and Uzbekistan use certain Chinese-style models of cybersecurity, which include sophisticated monitoring of online activity. Russia's role as a regional cybersecurity partner is characterized by the sharing of technical expertise.

Several challenges hinder the development of a unified and comprehensive cybersecurity system in Central Asia. These include:

Lack of technical expertise. The lack of qualified cybersecurity professionals in the region makes it difficult for countries to develop and implement effective cybersecurity strategies. Governments often rely on foreign experts and external funding, which limits the sustainability of cybersecurity measures.

Insufficient investment. The level of investment in cybersecurity infrastructure varies significantly across the region. While Kazakhstan and Uzbekistan have invested significantly, countries such as Turkmenistan and Tajikistan have yet to fully fund their cybersecurity programs.

There is significant potential for regional cooperation in addressing cybersecurity challenges in Central Asia. The establishment of cross-border cybersecurity networks, threat intelligence-sharing platforms, and regional cybersecurity training programs could strengthen collective defense against cyber threats.

Efforts to establish a Central Asian cybersecurity framework as a regional mechanism for cooperation on cybersecurity policy, threat intelligence, and capacity-building could help improve the region's overall security posture. This will also lead to the development of common cybersecurity standards and guidelines across the region.

CONCLUSION

Cybersecurity in Central Asia is still in its infancy, but has made significant progress in recent years. While countries such as Kazakhstan and Uzbekistan have developed comprehensive national cybersecurity strategies, others face significant challenges in infrastructure, governance, and capacity building. The region's geopolitical dynamics, lack of technical expertise, and fragmented legal frameworks complicate efforts to strengthen cybersecurity.

However, regional cooperation and international partnerships offer significant opportunities to strengthen the cybersecurity landscape in the countries of the Central Asian region. Governments, industry stakeholders, and international organizations must work together to address these challenges, share best practices, and invest in the region's digital future.

References:

1. Almazov, A., & Dastanov, I. (2020). Cybersecurity in Central Asia: Challenges and Opportunities. Journal of Central Asian Studies, 17(3). P. - 202-221.
2. Bo'tayev U.X., Turdiyev U.R. Markaziy Osiyo mintaqasida kiberxavfsizlik. Monografiya. – T.: 2024. – B.32.
3. Cybersecurity Cooperation in Central Asia. (2022). *Regional cooperation in the fight against cybercrime: A case study of Central Asia's cybersecurity collaboration*. International Journal of Cyber Policy, 14(3). P. - 124-140. https://doi.org/10.1007/s40753-022-00125-7
4. Gobal Cybersecurity Index 2017. Geneva: International Telecommunication Union (ITU), 2018. – P.118.
5. Ибрагимова Г. Подходы государств Центральной Азии к вопросам управления интернетом и обеспечения информацонной безопасности // Индекс безопасностиб 20136 № 1.-С.103-128

6. Концепция информационной безопасности Кыргызской Республики на 2019-2023 годы (к Постановлению Правительства КР № 209 от 3 мая 2019 года). URL: cbd.minjust.gov.kg/act/view/ru-ru/13652 (дата обращения: 19.02.2020).

7. Кульжанова Г. Некоторые аспекты проблемы политической модернизации местного государственного управления // Казахстан-Спектр, 2005 – № 2. – С.22

8. Markaziy Osiyoda mushtarak jihatlar, tahdidlar va yangi imkoniyatlar. O'zbekiston Respublikasi Prezidenti huzuridagi Strategik va mintaqalararo tadqiqotlar instituti, 16.02.2019. http://uza.uz/oz/society/markaziy-osiyoda-mushtarak-zhi-atlar-ta-didlar-va-yangi-imko-15-02-2019

9. Я.Ибодов А.Х. Информационная безопасность: новые вызовы и угрозы в процессе перехода к информационному обществу (на материалах Республики Таджикистан): Дис. канд. полит. наук.- Душанбе.: 2015. - С.32

10. Закон Туркменистана "О правовом регулировании развития сети Интернет и оказания интернет-услуг в Туркменистане" от 20 декабря 2014 г., № 159-V// http://www.wipo.int/wipolex/ru/text.jsp?file_id=398876