Journal DOI: 10.36713/epra1013 | SJIF Impact Factor (2025): 8.619 ISSN: 2347-4378
EPRA International Journal of Economics, Business and Management Studies (EBMS)
Volume: 12 | Issue: 9 | September 2025 -Peer-Reviewed Journal

CYBER SECURITY AND PUBLIC DEBT: RISK MANAGEMENT IN THE CONTEXT OF DIGITAL TRANSFORMATION

Tilabov Nasrulla Tashmuratovich
Tashkent State University of Economics,Finance and Financial Technologies Department,
Associate Professor, PhD
ORCID 0000-0002-4412-4019

ABSTRACT
This article explores the issues of risk management in the areas of cyber security and public debt in the era of digital transformation. At the same time, an increase in the volume of public debt and the introduction of new digital solutions in its management are putting operational risks, including risks associated with cybersecurity, on the agenda. The article examined scientific approaches to this problem through the analysis of research conducted by scientists from Uzbekistan and foreign countries. Proposals for minimizing risks were also developed, analyzing the impact of cyber threats on economic stability and stability of public debt in the context of digitization of Public Finance.
KEYWORDS: *Cyber Security, Public Debt, Digital Transformation, Risk Management, Digital Economy, Cyber Threats, Operational Risk.*

INTRODUCTION

Digital transformation is the process of achieving efficiency through the widespread introduction of information and communication technologies (ICT) in the economy and public administration. Today, both in the world and in Uzbekistan, digitalization is accelerating in all areas. However, the transition to digital systems poses a number of new risks. In particular, it is observed that the digitalization of economic processes creates opportunities for cybercrime and increases the number of cyber threats such as financial fraud and data theft.

The issue of cybersecurity is becoming more relevant in the process of introducing digital technologies into the public administration and financial system. In the context of a digital economy, public debt management is also based on modern information and communication technologies: for example, placing bonds through electronic auctions, automating state financial reporting, etc. In such conditions, cybersecurity threats can also directly affect the financial stability of the state. For example, experts emphasize that as a result of a large-scale cyberattack, the country's economy may collapse, financial institutions may be paralyzed, and additional costs may be imposed on the state.

In recent years, the world has seen an unprecedented increase in the scale of cybercrime. According to research, the amount of damage caused by global cybercrime in 2021 was estimated at 6 trillion US dollars, and by 2025 this figure is projected to reach 10.5 trillion US dollars annually. These figures mean that the economic damage caused by cyberattacks exceeds even the damage caused by major natural disasters or the illegal drug trade. Neglecting cybersecurity can have serious consequences not only for the private sector, but also for public finances. [1]

In the case of Uzbekistan, a number of state programs are being implemented to develop the digital economy.
At the same time, significant changes have been observed in the volume and composition of public debt in Uzbekistan in recent years. According to the latest data, as of July 1, 2025, Uzbekistan's public debt reached $ 43.3 billion. $ 36.4 billion of public debt is external debt, $ 6.9 billion is internal debt. Public debt increased by $ 6 billion compared to the same period last year. Its share in GDP also increased by 1.8 percentage points, from 32.4 percent to 34.2 percent.

For comparison, as of July 1, 2024, public debt amounted to $ 37 billion 241 million. This indicator increased by 16.5 percent in one year. Therefore, the issue of ensuring the stability of public debt is urgent, and it is necessary to take into account new types of risks. [2]

Journal DOI: 10.36713/epra1013 | SJIF Impact Factor (2025): 8.619 ISSN: 2347-4378
EPRA International Journal of Economics, Business and Management Studies (EBMS)
Volume: 12 | Issue: 9 | September 2025 -Peer-Reviewed Journal

LITERATURE REVIEW

Research on public debt and financial risk management. There is extensive scientific literature on the consideration of various risks in public debt management. In the traditional approach, financial risks such as interest rate risk, exchange rate risk, refinancing risk, and liquidity risk are the main focus for the public debt portfolio. In the manuals of international organizations, measures such as optimizing the composition of debt, diversifying its terms, and limiting currency risks are recommended to maintain a safe level. In the case of Uzbekistan, economists have also highlighted the issues of effective public debt management. In particular, M. Mirzamakhmudov (2023), analyzing the expansionary fiscal policy and public debt dynamics of Uzbekistan in recent years, also shows the impact of the digital economy on the stability of public debt. In his opinion, it is possible to increase the efficiency of borrowed funds and ensure sustainable growth by developing the digital economy and expanding public-private partnership (PPP) projects. This approach aims to reduce poverty and achieve economic growth through the rational use of public debt. [3] Also, economist N. Tilabov, in his article "Directions for expanding the possibilities of using Islamic financial instruments in optimizing public debt policy," has views on the fact that diversification in public debt policy - the use of Islamic financial instruments along with traditional debt instruments - serves to stabilize the debt burden. [4]

At the same time, recently, attention has also been increasing on the topic of operational risks in public debt management. The World Bank and other organizations, raising the issue of ensuring the discipline and continuity of execution of public debt, emphasize the need for special contingency plans for debt management offices (DMOs). In particular, in the context of the pandemic of 2020-2021, it became clear that many countries lacked sufficient contingency plans in their debt management systems. When the World Bank studied the situation in 65 countries, it was found that many countries lacked business continuity and disaster recovery plans, especially weaknesses in cybersecurity and data protection. This situation confirms that, as noted above, cybersecurity risks are also relevant in debt management. [5]

Foreign expert D. Hidi (2023) also speaks about operational risks in the debt management system, highlighting the issue of ensuring cybersecurity. He notes that during the pandemic, debt agencies have become more dependent on technology as they have moved to remote work, and as a result, the risk of cyberattacks such as data leaks, phishing (email fraud), and malware has increased dramatically. The problem is that cyberattacks can disrupt debt operations, for example, the inability to hold an electronic bond auction or delay debt payments. As a result, if the state is unable to raise money from the financial market or service its debt at the right time, this is considered a default risk and has a negative impact on its credit rating. Indeed, there are examples of debt payments being delayed in some countries due to technical failures or operational disruptions, which are considered sovereign defaults by international rating agencies. For this reason, international organizations recommend that countries develop contingency plans for unexpected risks (including cyber threats) in debt management. [6]

From the above literature analysis, it can be seen that in the era of digital transformation, the issue of cybersecurity is gaining strategic importance not only from the point of view of information technology or national security, but also from the point of view of financial stability and public debt sustainability. In the current situation, it is an urgent task for countries like Uzbekistan to study international experience in the process of integrating into the digital economy, strengthen their national cybersecurity infrastructure, and prepare the public finance system for new threats.

METHODOLOGY

This study used a systematic analysis and comparative approach. First, domestic and foreign scientific literature, reports and articles on the topic were studied, and an attempt was made to identify the intersection points between cybersecurity and public debt management. Then, through the analysis of secondary data, global and national trends were compared: statistics of cyber attacks, their economic consequences, dynamics and composition of the public debt of Uzbekistan, recommendations of international rating agencies were studied.

During the study, regulatory and legal documents and official information were also reviewed: decrees and resolutions of the President of the Republic of Uzbekistan (in particular, the "Digital Uzbekistan – 2030" strategy and the law "On Cybersecurity"), materials of the Ministry of Finance of Uzbekistan and the Ministry of Digital Technologies, reports and instructions of international financial institutions (IMF, World Bank, Asian Development Bank) were analyzed. An attempt was also made to quantitatively assess the state of the problem based on statistical data. The results were presented using tables and graphs.

Journal DOI: 10.36713/epra1013 | SJIF Impact Factor (2025): 8.619 ISSN: 2347-4378
EPRA International Journal of Economics, Business and Management Studies (EBMS)
Volume: 12 | Issue: 9 | September 2025 -Peer-Reviewed Journal

The research methodology was mainly descriptive and analytical in nature, in which conclusions were drawn through the analysis of data obtained from open sources. All figures and facts cited were taken from reliable sources, and relevant references to them were provided throughout the article.

RESULTS

1. Trends in Cybersecurity Threats in the Era of Digital Transformation First, let's look at the main indicators that indicate the state of cybersecurity on a global scale. Selected Table 1 presents some data on the statistics of cyberattacks and their economic losses in the world and Uzbekistan.

Table 1

Global and local cybersecurity indicators [7]

Indicators	Amount (year)
Global annual cybercrime damage	$6 trillion (2021) – $10.5 trillion (2025 forecast)
Number of major cyberattacks worldwide	1120 (2020)
Volume of compromised (stolen) data (worldwide)	20 billion+ records (2020)
Detected malicious attacks in Uzbekistan (2020)	27 million+
Cyber incidents recorded in Uzbekistan (2020)	342

As can be seen from the table above, the scale of threats in the field of cybersecurity is growing at an unprecedented rate. Billions of data are being stolen around the world, thousands of major cyberattacks are being carried out. The more than 27 million malicious and suspicious attacks detected in the territorial Internet segment of Uzbekistan in 2020 also show how relevant this area is for our country. Meanwhile, in 2021, global cybercrime caused $6 trillion in damage, and this figure is likely to exceed $10 trillion per year by 2025, which is alarming the world community.

In Uzbekistan, too, cybersecurity has recently been receiving special attention. By the Resolution of the President of the Republic of Uzbekistan No. PQ-4452 dated September 14, 2019 “On additional measures to improve the system of control over the implementation of information technologies and communications, their protection”, the State Enterprise “Cybersecurity Center” [8] was established and security audits of information systems of state bodies were launched. The Law of the Republic of Uzbekistan “On Cybersecurity” No. O'RQ-764 dated April 15, 2022 [9], adopted in 2022, established obligations to ensure information security in the state and private sectors. These and a number of other regulatory documents and institutions on cybersecurity serve to shape state policy against emerging threats in the digital environment.

In this regard, according to the 2023 report of the State Enterprise "Cybersecurity Center", cyber attacks on web resources increased by 148% compared to 2022. That is, in 2022 there were 4,433,789, while in 2023 there were 11,020,235 cyber attacks.

Also, according to the center's report, the largest number of cyber attacks was observed in the Netherlands with 759,502, in the USA with 696,671, in Russia with 100,549, in Germany with 58,375, in India with 53,495, in China with 51,667, in Georgia with 32,137, in Kyrgyzstan with 23,375, in Finland with 21,958 and in Hong Kong with 21,034. [11]

2. The impact of cyber threats on public debt management Let us now consider how the issue of cybersecurity directly relates to public debt. First of all, let us recall that public debt management is increasingly relying on digital infrastructure. Currently, many countries use electronic trading platforms to place their foreign and domestic debt, allowing investors to buy government bonds online, and debt settlements are carried out in real time through electronic systems. For example, the World Bank has even issued bonds using blockchain technology, and transactions with these financial instruments are managed on the basis of a fully digital registry. Since 2018, the Austrian Public Debt Agency (Oesterreichische Bundesfinanzagentur) has introduced the practice of notarizing transaction reports at government bond auctions using blockchain. Officials say that this solution has increased the transparency and security of the auction process and strengthened investor confidence. [10]

The introduction of digital solutions unfortunately also introduces new risks. The most dangerous scenario for public debt management is the interruption or incorrect execution of debt operations due to a cyberattack on information systems. Such situations can lead to negative consequences through several channels:

- Disruption of financial operations:
- Interruptions in the payment system:
- Corruption or loss of data.

The above situations are dangerous scenarios, and government agencies are taking special measures to prevent them. For example, a number of countries have developed special business continuity plans in their debt management offices (DMOs), which specify an alternative (manual) auction or payment procedure in the event of a breakdown of electronic systems. According to the World Bank, each country's debt management system should be stress-tested at least once every two years and backed up regularly. Many developed countries are organizing centralized cyber training grounds and conducting special training exercises with the participation of various agencies to protect their national financial systems from cyber threats. For example, the European Central Bank has been organizing multi-country simulation games called "EU Cyber 202X" [12] to practice an interbank cyber attack scenario.

3. When analyzing the risk analysis in the context of Uzbekistan, the above global risks are not alien to Uzbekistan. In recent years, our country has actively entered international financial markets and launched the placement of government securities. In particular, in 2019, Uzbekistan successfully carried out the first international sovereign bond (Eurobond) issue. Today, Uzbekistan's international bonds are traded on the London Stock Exchange through an electronic trading system. In the domestic market, the Ministry of Finance has also been selling state treasury bonds through electronic auctions since 2020. All of these processes rely on ICT infrastructure, and their uninterrupted operation is important for state finances.

The Treasury information systems under the Ministry of Finance and the payment and clearing system of the Central Bank are considered the basis of the country's financial stability. Currently, measures have been taken to ensure cybersecurity in these systems, and the responsible agencies (DSX, Ministry of Information Technologies, etc.) are issuing methodological instructions to financial institutions. At the same time, work in this area needs to be further strengthened. For example, the draft Strategy for the Development of the Digital Economy of the Republic of Uzbekistan until 2030 sets out measures to protect large information systems from modern cyber threats and implement a coordinated cybersecurity policy. If we analyze the public debt portfolio of Uzbekistan, as of 2023, about 60% of the total debt will be external (in foreign currency) debts. While this poses currency risks, from a cybersecurity perspective, most debts are managed electronically with international financial institutions and creditors. Therefore, the uninterrupted operation of international payment systems (SWIFT, etc.) and secure channels for exchanging information with creditors are of particular importance in public debt management. Therefore, the Central Bank of Uzbekistan and commercial banks are taking measures to strengthen their payment systems and SWIFT infrastructure.

Turning to significant cyber incidents that have occurred in our country, the media reported, for example, in 2021, that attempts to gain unauthorized access to the database of one of the largest banks were reported. Law enforcement agencies and relevant CERT services reported that they detected and eliminated such attacks in a timely manner. Although these cases have not yet led to serious financial losses, it indicates that inaction may be costly in the future.

In general, cybersecurity is a high priority among the risks associated with the transition to a digital economy in Uzbekistan. A comprehensive approach to managing operational and cyber risks is necessary to strengthen the stability of the public financial system.

CONCLUSION

In the era of digital transformation, the connection between cybersecurity and public debt is becoming increasingly strong. The above analysis shows that these two areas, which at first glance are separate areas, are actually of common importance for the economic stability and financial security of the country. Without ensuring cybersecurity, it is difficult to ensure the continuous and reliable operation of the state finance system, which is being formed on the basis of the digital economy. Similarly, ignoring new digital risks when conducting a public debt strategy can lead to the failure of financial plans.

Based on the scientific sources and real examples studied in the article, the following conclusions and proposals are put forward:

1. Deciding on cybersecurity as a national priority.

2. Taking operational risks into account in public debt management.
3. Modernizing information systems and reducing "technical debt".
4. Training qualified personnel in cybersecurity.
5. International cooperation and exchange of experience.

In conclusion, it should be noted that digital transformation is a requirement of development, it is impossible to lag behind it. However, anticipating and managing new risks emerging in the process of digitalization is very important for the country's economic security. Investments and reforms aimed at ensuring cybersecurity may currently have a certain impact on the increase in public debt, but in the future these measures will prevent huge losses that may occur. In this sense, every soum spent on cybersecurity should be considered a strategic investment in maintaining the stability of public finances.

Consistent implementation of the above recommendations is important for Uzbekistan to successfully manage cybersecurity and public debt risks on its path to a digital economy. This, in turn, will serve to strengthen the economic development and financial sovereignty of our country.

REFERENCES

1. *Cybersecurity Ventures (2020). "Cybercrime To Cost The World $10.5 Trillion Annually By 2025" – Cybersecurity Magazine maxsus hisobotidan lavha. https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/.*
2. *O'zbekistonning davlat qarzi 43 mlrd dollardan oshdi. Bu pullar nimaga ishlatilgan? https://kun.uz/kr/32478167*
3. *Mirzamakhmudov M. (2023). "Public Debt of Uzbekistan: The Role of Global Financial Institutions in the Development of Economic Activities" – American Journal of Innovative Research and Applied Sciences, Vol. 7, Issue 6, 2023. https://www.american-ajiras.com/Marufjon%E2%80% 93Ref1-6-16ajira070623.pdf*
4. *Tilabov N. "Davlat qarz siyosatini optimallashtirishda islomiy moliya instrumentlarining qo'llanish imkoniyatlarini kengaytirish yo'nalishlari". "Yashil iqtisodiyot va taraqqiyot" jurnali. 2025 y. 9-son.299-304 betlar.*
5. *Debt Management Office (DMO). https://www.dmo.gov.uk/*
6. *Hidi D. (2023). "Operation Resilience: Why Public Debt Management Offices Need Business Continuity And Disaster Recovery Plans" – BCI (Business Continuity Institute) Blog, 15-may 2023 y.[11][12][23]. https://www.thebci.org/news/bcaw-2023-operation-resilience-why-public-debt-management-offices-need-business-continuity.html*
7. *Cybercrime To Cost The World $10.5 Trillion Annually By 2025.*
8. *https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/*
9. *Resolution of the President of the Republic of Uzbekistan No. PQ-4452 dated September 14, 2019 "On additional measures to improve the system of control over the introduction of information technologies and communications, their protection". https://lex.uz/uz/docs/-4665548*
10. *Law of the Republic of Uzbekistan No. O'RQ-764 dated April 15, 2022 "On Cybersecurity". https://lex.uz/uz/docs/-5960604*
11. *State Enterprise "Cybersecurity Center". https://csec.uz/uz/news/ maqolalar/o-zbekiston-respublikasi-kiberxavfsizligi-2023-yil-hisoboti/*
12. *Public Debt Management: Is the future closer than we think? https://blogs.worldbank.org/en/voices/public-debt-management-future-closer-we-think*
13. *"EU Cyber 202X". https://digital-strategy.ec.europa.eu/en/policies/ cybersecurity-strategy*
14. *Data from the Ministry of Economy and Finance of the Republic of Uzbekistan, the Central Bank, the International Monetary Fund, and the World Bank were used. (2020-2025).*