


## CYBERSECURITY IN UZBEKISTAN: PROTECTING THE DIGITAL ECONOMY

**Karshieva Nilufar Tovboy kizi**

MBA student, Inha University in Tashkent

karshiyeva.nilufar6789@gmail.com <https://orcid.org/0009-0008-4480-5480>

Article Info	ABSTRACT
<p><b>Article history:</b> Received May 21, 2024 Revised Jun 10, 2024 Accepted Jun 17, 2024</p> <p><b>Keywords:</b> cybersecurity, digital economy, economic development, cybersecurity law, cyber risks</p>	<p>Strong cybersecurity standards are more vital than ever as Uzbekistan's digital economy continues to flourish. This article examines the current state of the country's cybersecurity infrastructure, identifying significant risks and flaws that affect both individuals and businesses. It also underlines how the public and private sectors have collaborated to strengthen cybersecurity and create a safe online environment that fosters growth and innovation. By evaluating these components, we may gain a comprehensive understanding of the challenges and preventative measures driving Uzbekistan's strategy for safeguarding its constantly increasing digital environment.</p> <p>This is an open-access article under the <a href="#">CC-BY 4.0</a> license.</p> 

**Corresponding Author:**

**Karshieva Nilufar Tovboy kizi**

MBA student, Inha University in Tashkent

Email: karshiyeva.nilufar6789@gmail.com

### INTRODUCTION

Uzbekistan's internet landscape has shifted dramatically during the last decade. The digital economy, which includes e-commerce, digital banking, online services, and other activities, has emerged as a key driver of the country's economic development. However, with tremendous expansion comes a big challenge: cybersecurity. As Uzbekistan's economy continues to digitalize, the necessity of strong cybersecurity measures cannot be stressed. Cyber dangers are changing at an unprecedented rate, and safeguarding sensitive information and key infrastructure is more important than ever.

### Historical Context

Uzbekistan's journey to a digital economy began in the early 2000s, when the government recognized the power of information and communication technology (ICT) to fuel economic growth and development. The foundation of the Ministry for Development of Information Technologies and Communications in 2015 marks an

important turning point in this path. The ministry was given the responsibility with developing and carrying out policies to encourage the use of ICT in various areas such as government, education, healthcare, and business.

### **Current Trends**

Today, Uzbekistan's digital economy is growing. The rapid usage of cellphones and the internet has transformed how people interact, obtain information, and do business. E-commerce platforms have grown in popularity, providing consumers with a comfortable online shopping experience. Digital banking services have made financial transactions more convenient and efficient. The government has also embraced digital change, launching projects like e-government services to improve public service delivery and transparency.

### **The Growing Cyber Threat Landscape**

A wider range of cyber dangers is facing Uzbekistan as a result of the country's rising internet access and increasing number of digital services. Targeting both the public and private sectors, cybercriminals, hacktivists, and state-sponsored actors take advantage of weaknesses in digital infrastructure. Ransomware, phishing, malware, and data breaches are examples of common cyberthreats that can cause financial losses, interrupt services, and compromise sensitive data.

In addition, because of the global digital economy's mutual dependence, cyber risks are not limited by state boundaries. Cyberattacks in one area of the world may carry over to other areas, including Uzbekistan. The significance of global collaboration and information exchange in addressing cyber threats is emphasized by this interconnection.

### **The Legal Framework: Uzbekistan's First Cybersecurity Law**

In April 2022, Uzbekistan took a significant step by adopting its first Law "On Cybersecurity" (No. LRU-764) [1]. This legislation, which comes into force on July 17, 2022, aims to enhance cybersecurity practices across various sectors. Key provisions of the law include:

1. **Critical Facilities:** The law covers those who operate vital facilities, which include those in the public administration, military, energy, and other sectors. The regulator's cybersecurity requirements must be fulfilled by these operators.
2. **Obligations for Critical Facility Operators:**
  - Implement cybersecurity requirements set by the regulator.
  - Ensure continuous operation of critical facilities.
  - Store data (with backup copies) for at least the last three months.
  - Certify hardware, firmware, and software.
  - Install monitoring systems to prevent cyber-attacks and respond to incidents.
  - Comply with regulator instructions to rectify violations.
  - Prevent unauthorized access and data loss.
  - Report incidents and cybercrimes promptly.

3. **Regulatory Oversight:** The Office of the President establishes unified public policy pertaining to cybersecurity, while the State Security Service of Uzbekistan acts as the regulator in this area.

4. **Challenges and Opportunities:** Every year, Uzbekistan is subject to more than 1.3 million cyberattacks [2]. The number of active domains with security certificates is now only 14,000, thus strengthening defenses is important. But this also offers qualified individuals a chance to improve the cybersecurity environment in the nation.

Even while Uzbekistan has achieved great strides, there are still obstacles in the way of its efforts to protect its digital economy. These difficulties include the increasing speed of technical advancement, the dynamic character of cyberthreats, and the ongoing need to invest in cybersecurity personnel and equipment. By utilizing a range of strategies including public-private partnerships, workforce development, international cooperation, and government initiatives, Uzbekistan can establish a strong cybersecurity framework that will guarantee the prosperity and security of its digital future.

## **2. Current State of Cybersecurity Infrastructure**

### **An overview of Uzbekistan's digital landscape.**

Inadequate cybersecurity measures are Uzbekistan's biggest cross-cutting obstacle in growing its digital environment. Although the Government Cybersecurity Center has a competent staff of experts, its resources are still limited and are mostly focused on protecting vital government systems. Unfortunately, major state-owned companies, local governments, private companies, groups, and people are not aware of cybersecurity dangers or have the necessary skills to properly handle them. Few businesses are involved in the cybersecurity sector due to the lack of demand for these services [3].

### **Global ranking of cybersecurity**

Uzbekistan ranked 94th in the 2023 National Cyber Security Index (NCSI), out of a total of 176 countries. This index was created by experts from the Estonian Academy of Electronic Governance. Since the start of the year, Uzbekistan has fallen from 89th to 94th place, having been 88th at the end of 2022. The NCSI considers factors such as the global cybersecurity index, the development of information and communication technologies, and the network readiness rating. Among Central Asian countries, Kazakhstan achieved the best result, ranking 78th, followed by Kyrgyzstan (91st), Uzbekistan, Tajikistan (153rd), and Turkmenistan (164th). Globally, Belgium, Lithuania, and Estonia are the most secure against cyber threats, while the Federated States of Micronesia, Palau, and South Sudan have the poorest rankings [4].

### **Mention key organizations or bodies responsible for cybersecurity.**

UzCERT (Uzbekistan Cybersecurity Emergency Response Team) is a component of Uzbekistan's Cybersecurity Center, a state-owned company under the direction of the State Security Service. Its placement under the State Security Service underlines the government's prioritizing of cybersecurity as a state security issue rather than a more general concern for the digital ecosystem, even though it is formally responsible for

working with both the public and private sectors. The Cybersecurity Center is responsible for a wide range of tasks, such as gathering and evaluating data on threats to information security, liaising with law enforcement and telecom providers, inspecting and approving hardware and software, supporting government agencies in the creation of security policies, suggesting changes to regulations, and alerting the public to new threats. The Center provides cybersecurity investigations of websites with the ".UZ" domain, data recovery, penetration testing, security audits, and information system compliance inspections. Its main priority has been to protect vital government systems. The Cybersecurity Center maintains bilateral ties with nations such as South Korea, the UAE, Poland, Japan, Malaysia, India, and Russia in addition to working with a number of multilateral organizations. According to cybersecurity experts, the Center frequently uses Russian expertise for training, while hardware solutions are supplied by American, Israeli, and European businesses (such as Cisco, Fortinet, Checkpoint, and Juniper) [3, 5].

#### **Challenges faced in maintaining and updating cybersecurity measures.**

A somewhat undeveloped area of the digital economy in Uzbekistan is cybersecurity. The public's low level of cybersecurity knowledge and inability to spot online and digital payment fraud prevents the financial sector from using additional digital solutions. Consumer faith in digital financial services is being undermined by a rise in fraud, system disruptions, and data breaches. To improve cybersecurity policies and practices, the financial services industry must encourage cooperation between all players, including banks, mobile money providers, other third-party providers, and regulators [3].

### **3. Key Threats and Vulnerabilities**

#### **Common Cyber Threats**

Although the rapid integration of digital media has led to numerous advantages, the citizens of Uzbekistan might be particularly vulnerable to the dangers that come with it. There is a marked lack of public understanding regarding data rights, cybersecurity dangers misinformation, disinformation, and online safety. Interviews reveal that public education on these problems has not been given priority by the government. Merely 12,500 out of the 86,679 ".uz" registered domains has SSL security certificates. In a single year, around 11% of Uzbek internet bank users were the target of malicious software or viruses, according to the Kaspersky Lab Bulletin 2020 [4]. A few years ago, the online game "Blue Whale" allegedly encouraged teen suicide, which brought attention to child internet protection and resulted in a law protecting kids from dangerous content. Still lacking, though, is a systematic method to teaching kids, parents, educators, and the general public about the dangers of cyberbullying and online harassment [7].

#### **Discuss the most critical vulnerabilities in the digital economy**

The government's efforts have mostly addressed issues related to national security, ignoring the wider social and economic effects of subpar cybersecurity. As seen by Uzbekistan's declining standing in different worldwide indices, this lack of resources

and commitment has left the country's cybersecurity systems immature, leaving many government systems, enterprises, organizations, and individuals insecure. Experts from the area observe that the Cybersecurity Center does not have enough resources or highly qualified technical personnel to do its duties. The majority of information security specialists have obtained training overseas, and TUIT University is the only university in Uzbekistan that offers a degree in this field. Thus, as demonstrated by multiple high-profile cyberattacks in 2021, such as the Clone Security Group's hacking of regional authority websites, non-essential government systems continue to be susceptible.

Although the Cybersecurity Center is in charge of training and capacity building, it offers little services in these areas, which causes enterprises, organizations, and the general public to have low cybersecurity knowledge and capacity. Other parties occasionally organize cybersecurity events. Examples include seminars hosted by Kaspersky Lab and the Central Bank of Uzbekistan, as well as a one-day event organized by UZCARD Ventures. Companies that provide cybersecurity consulting services include Mars Solutions, Expert Pro, Sharifa, Softline, and Jet Infosystems; however, because of the general lack of awareness regarding cybersecurity, their ability to operate is restricted. While services for regulatory compliance and employee training are still in the early stages of development, these organizations primarily concentrate on safeguarding IT perimeters and building layered protection. As far as Uzbekistan is concerned, no business has received ISO 27001 certification for information security. Furthermore, the private sector does not sufficiently address industry demands in data science, cybersecurity, and machine learning. Instead, it provides a restricted curriculum focused mostly on coding and programming.

#### **The potential and actual impacts of these threats and vulnerabilities on businesses and the economy.**

In Uzbekistan, e-commerce and digital trade encounter many obstacles. A poor e-commerce culture, outdated trade and customs laws, and limitations in the infrastructure of distribution, logistics, and transportation are major obstacles. Development is further hindered by the lack of regulations around the use of remote identification systems and by the inadequate telecom infrastructure, particularly with regard to the low penetration of broadband mobile internet in rural areas. A common weakness in consumer digital literacy and cybersecurity knowledge leads to a rise in online fraud involving online transactions. In addition, the e-commerce industry lacks the skilled labor necessary to maintain its growth and global expansion [3,9].

#### **4. Government and Private Sector Efforts to Enhance Cybersecurity**

##### **Government Initiatives**

The Oliy Majlis Senate debated an act that will improve cybersecurity by modifying a number of existing laws. This law gives the Central Bank more authority to recognize and counteract security threats from financial organizations, with the goal of enhancing information security, especially in credit and non-bank credit institutions. The revisions designate infractions inside banking information systems as significant



offenses and involve legislation connected to the Central Bank, banking activities, bank secrecy, automated banking systems, electronic government, and payments. With the goal of enhancing information security, enabling a secure e-government system, and preventing cybercrimes, the emphasis is on safeguarding banks' information systems and maintaining bank confidentiality. Senators think that Uzbekistan's financial sector's cybersecurity measures will be much improved by this bill [11].

#### **Examples of government-led cybersecurity programs or training initiatives.**

By offering training in IT, digital literacy, and cybersecurity, the Digital Uzbekistan Strategy highlights the significance of enhancing digital literacy and skills among regional governors, administration officials ("Khokimyat"), and staff members of state agencies and organizations. The aim is to train twelve thousand workers.

Managers in the private sector are becoming more aware of cybersecurity dangers as a result of a few recent public occurrences. However, due to a lack of local knowledge in cybersecurity and information security, businesses frequently need to engage cybersecurity specialists from other nations, most notably Russia. Since 2020, TUIT has seen a growth in enrollment in its Faculty of Information Security, recognizing the growing demand for local expertise.

Furthermore, MITC-backed OSCE Uzbekistan and Softline Education have started an initiative to offer both basic and advanced cybersecurity training. The project's target audience includes cybersecurity line managers and technicians, heads of departments, ministries, businesses, and instructors at specialist educational institutions [3].

#### **Private Sector Contributions**

With assistance from Kaspersky Lab, Universoft IT LLC is introducing the first domestically produced antivirus program in Uzbekistan. Through this agreement, Uzguard AV software will be launched, employing the technologies of Kaspersky Lab and being certified to fulfill national criteria in Uzbekistan. By concentrating on high-tech import substitution and creating cutting-edge national products, Universoft IT seeks to strengthen technological sovereignty [12].

#### **Insights into the future of cybersecurity in Uzbekistan.**

The cybersecurity industry in Uzbekistan is expected to grow significantly, according to Statista. The market is expected to generate US\$72.30 million in revenue by 2024, with Cyber Solutions leading the way at US\$45.04 million. It is anticipated that the market will expand at a yearly pace of 14.74%, with a potential value of US\$143.80 million by 2029. According to estimates, Uzbekistan will invest \$4.99 on cybersecurity on average per employee by 2024. Despite their rapid expansion, the United States is predicted to account for the majority of global cybersecurity revenue in 2024—US\$81,370.0 million. Due in large part to weaknesses revealed during the COVID-19 crisis, cybersecurity has moved from being the purview of the IT department to becoming an essential part of top-level strategic planning [13].

## CONCLUSION

It is impossible to overestimate the significance of strong cybersecurity measures as Uzbekistan continues to embrace the digital economy. Significant economic potential have resulted from the quick development of digital platforms and services, but the country is now vulnerable to a wide range of cyberthreats and vulnerabilities. In order to safeguard the digital economy and promote sustainable growth, Uzbekistan needs to take proactive measures to improve its cybersecurity environment.

To ensure the growth and protection of Uzbekistan's digital economy, the following steps should be taken:

### Strengthen Cybersecurity Infrastructure:

- Increase funding and resources for the Cybersecurity Center to enhance its capacity and capabilities.
- Implement advanced cybersecurity technologies and solutions to protect critical infrastructure and digital assets.

### Enhance Public Awareness and Digital Literacy:

- Launch nationwide campaigns to raise awareness about cybersecurity risks and best practices.
- Integrate cybersecurity education into school curricula and provide training programs for the general public.

### Foster Cybersecurity Startups and Innovation:

- Create incentives and support programs for cybersecurity startups to encourage innovation and entrepreneurship in the sector.
- Establish cybersecurity incubators and accelerators to nurture new ideas and solutions.

### Promote Public-Private Partnerships:

- Encourage collaboration between the government and private sector to share knowledge, resources, and best practices.
- Develop joint initiatives and projects to address common cybersecurity challenges.

### Improve Regulatory Framework:

- Update and strengthen cybersecurity laws and regulations to address emerging threats and vulnerabilities.
- Ensure compliance with international cybersecurity standards and best practices.

### Invest in Cybersecurity Research and Development:

- Support research and development efforts to advance cybersecurity technologies and solutions.
- Collaborate with academic institutions and research organizations to drive innovation in the field.

### Build a Skilled Cybersecurity Workforce:

- Develop specialized training programs and certifications to build a skilled cybersecurity workforce.

- Encourage continuous professional development and upskilling for cybersecurity professionals.

Enhance Incident Response and Recovery Capabilities:

- Establish robust incident response and recovery plans to quickly address and mitigate cyber incidents.
- Conduct regular drills and simulations to test and improve response capabilities.

By implementing these measures, Uzbekistan can guarantee sustained economic growth in the digital era, safeguard its people and enterprises from cyberattacks, and create a robust and safe digital economy. Setting cybersecurity as a top priority will protect the country's digital assets and build confidence in the digital ecosystem, which will open the door to a successful digital future

## REFERENCES

- [1]. LAW OF THE REPUBLIC OF UZBEKISTAN ON CYBERSECURITY No. LRU-764, 15.04.2022. <https://lex.uz/uz/docs/6997403>
- [2]. More than 1.3 million cyberattacks detected in national internet segment in 2021, <https://kun.uz/en/news/2022/03/03/more-than-13-million-cyberattacks-detected-in-national-internet-segment-in-2021>
- [3]. DIGITAL ECOSYSTEM COUNTRY ASSESSMENT (DECA) Uzbekistan, JANUARY 2022, [https://www.usaid.gov/sites/default/files/2022-05/USAID\\_UzbekistanDECA.pdf](https://www.usaid.gov/sites/default/files/2022-05/USAID_UzbekistanDECA.pdf)
- [4]. [https://ncsi.ega.ee/country/uz\\_2022/](https://ncsi.ega.ee/country/uz_2022/)
- [5]. Uzcet.uz. Accessed October 22, 2021. <https://uzcert.uz/>.
- [6]. “Kaspersky Security Bulletin 2020. Statistics 2 Contents.” n.d. Accessed October 19, 2021. [https://go.kaspersky.com/rs/802-IJN-240/images/KSB\\_statistics\\_2020\\_en.pdf](https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2020_en.pdf).
- [7]. “Ministry of Internal Affairs: ‘Blue Whale’ Came to Uzbekistan Two Months Ago (МВД: ‘Синий кит’ пришел в Узбекистан два месяца назад).” 2017. Podrobno.uz. April 1, 2017. <https://podrobno.uz/cat/obchestvo/mvd-siniy-kit-prishel-v-uzbekistan-dva-mesyatsa-nazad/>.
- [8]. “Site of Surkhandarya Khokimiyat under Attack (Сайт хокимията Сурхандаръи подвергся атаке).” 2021. Gazeta.uz. January 6, 2021. <https://www.gazeta.uz/ru/2021/01/06/site/>.



- [9]. “Country Profile: Uzbekistan.” n.d. [www.nordeatrade.com](http://www.nordeatrade.com). Accessed October 21, 2021. <https://www.nordeatrade.com/en/explore-newmarket/uzbekistan/e-commerce>.
- [10]. [https://www.norma.uz/novoe\\_v\\_zakonodatelstve/prinyat\\_zakon\\_o\\_kiberbezopasnosti](https://www.norma.uz/novoe_v_zakonodatelstve/prinyat_zakon_o_kiberbezopasnosti)
- [11]. <https://nuz.uz/2024/06/25/kiberbezopasnost-v-uzbekistane-czentrobank-zadaet-standart/>
- [12]. [https://uza.uz/en/posts/kaspersky-lab-and-universoft-it-join-efforts-to-improve-the-level-of-cybersecurity-in-uzbekistan\\_559111](https://uza.uz/en/posts/kaspersky-lab-and-universoft-it-join-efforts-to-improve-the-level-of-cybersecurity-in-uzbekistan_559111)
- [13]. <https://www.statista.com/outlook/tmo/cybersecurity/uzbekistan>