ISSN 2047-3338

Cybercrime in Uzbekistan: Current Trends, Challenges, and Future Countermeasures

Shirin Komilova, Feruza Abdumannobova, and Debasis Das

Abstract— **The Republic of Uzbekistan is at a focal point in the digital era: the rapidity of technological adoption, the growing internet penetration, and the alteration in the economic facets place the nation in the spotlight of the prospects of digital transformation alongside the emergence of novel risks linked to the dynamic evolvement of cybercrime. Over the past few years, cybercrime in Uzbekistan has reached a critical peak of incidences with the number of cases of cyberattacks, financial fraud, phishing, ransomware, mobile malware and social engineering attacks on the rise. The increased infiltration of internet services, the spread of e-commerce, and the fast integration of the digital payment system have exposed individuals and organizations to cyber threats. The paper relies on the quantitative data reported by law enforcement agencies across the country, cybersecurity agencies, and international organizations and is supported by the qualitative data collected through interviews with IT specialists, government representatives, and victimized businesses. The present paper gives a detailed account of different kinds, origins, consequences and legal provisions of cybercrime in Uzbekistan. It also underscores the problems of law enforcement agencies and gives useful solutions as to how to react to cyber threats without compromising privacy and security.**

Index Terms— **Cybercrime, Cybersecurity, Uzbekistan, Digital Transformation, Cyber Policy and Central Asia**

I. Introduction

OVER the last few years, Uzbekistan has experienced accelerated digital transformation because of government efforts (Digital Uzbekistan 2030 strategy) in e-governance, e-commerce, online banking, smart infrastructure, and increasing the use of digital services in the public and private sectors. This shift has greatly boosted efficiency, transparency, and engagement of the citizenry in the economy but at the same time, this development has led to an increase in cybercrime. This trend is anchored on several factors. Law enforcers see that most frauds are founded on social engineering (e.g., phishing SMS or deceptive web sites) rather than technical intrusion: fraudsters tend to impersonate the representatives of legitimate organizations or governmental systems due to the ability to make citizens share PINs, codes, files.

The analysis of the trends in cybercrime in Uzbekistan prior to the COVID-19 pandemic and after the outbreak allows highlighting an impressive change in the magnitude and character of cybercrime. Before the pandemic, cybercrime was not that extensive, and the number of registered instances is around 863 in 2019, with the vast majority of these being phishing, intrusion into data, and simple online fraud.

Nevertheless, the fast digitalization of economic and social life in the periods of the pandemic and after it resulted in the dramatic increase of cyber incidents. According to statistics and reports of government officials and research, the cybercrime is increasing manifestly by 2024, the reported cases of cybercrimes had already escalated to almost 58,800 cases, which is an increase of 68 folds and comprised almost 44 per cent of all the crimes reported in the country [23]. Along with this growth was the mass adoption of online banking, e-commerce, and digital government services that posed a new threat that cybercriminals took advantage of with various tactics including bank-card fraud and social engineering attacks.

Over the past few years, the Uzbekistan country has witnessed a drastic increase in cybercrime as registered cases have more than increased by almost 68 times in a period of five years and losses amount to UZS 1.9 trillion. Although the expansion has been explained by the general increase in digital finance and online services domestically, several reported instances have highlighted the involvement of foreigners in the criminal ecosystem. It is worth noting that a cyber-fraud ring based in Tashkent comprised 11 foreigners and robbed more than 130 victims of almost UZS 3 billion. Similarly, cross-border operations of investigations between Uzbekistan and Belarus established that the volume of Belarus-related cyber-fraud cases related to Uzbek financial infrastructure increased to 142 in 2024 compared to 37 in 2023. Even though no such extensive data is available today that isolates the impact of the rising numbers of foreign visitors and residents on the prevalence of cyber-crime, such cases point to the idea that transnational actors and foreign national players are a

Shirin Komilova, Student, Computer Science Department, Webster University in Tashkent, Uzbekistan (Email: shirinkomilova1808@gmail.com).

Feruza Abdumannobova, Student, Computer Science Department, Webster University in Tashkent, Uzbekistan (Email: ferra18081112@gmail.com).

Debasis Das, Professor, Computer Science Department, Webster University in Tashkent, Uzbekistan (Email: debasisdas22583@gmail.com).

decent part of the changing cyber-threat environment in Uzbekistan.

Meanwhile, the nature of attacks continues to rise at a rate that is higher than the official response. As an example, the total loss of money in frauds in 2021-2024 constituted over 1.9 trillion Uzbek sum (= approximate value of 149 million) in frauds of which 603 billion was lost in 2024 (Wright, 2025). [20] The case of Uzbekistan does not represent an exception in the context of the region as a whole: the recent study of cybersecurity in Central Asia has identified Uzbekistan as a developing country when it comes to cybersecurity, although the nation, along with the neighboring state, needs to establish more explicit institutions and better implementation of ICT policies (Kaska, Maigre, and eGA, 2025, p. 9).

The research also examines the efficacy of the existing national cyber security policies and laws on tackling such threats. The paper suggests specific policy interventions, including capacity building on cyber law enforcement, better incident reporting systems, increased public education and awareness and cooperation between Uzbekistan and neighboring states, based on empirical evidence to enhance the cyber resilience. This paper adds to the existing knowledge on cybercrime in Central Asia and offers practical ideas to a policymaker, cybersecurity professionals, and academicians who want to reduce the risk of cybercrime in emerging economies.

This research paper will attempt to examine the current situation in cybercrime in Uzbekistan in the light of a multidisciplinary approach, by establishing key trends, institutional vulnerabilities and policy areas of intervention. The analyses of this intersection of technological advancement and online menaces make the research a part of the current discussion on the governance of cyber security in developing economies and an insightful piece of information, which can be reflected in the thinking of policymakers, businesses, and the scholarly community.

II. Internet Usage and Population Statistics in Uzbekistan (2015-2025)

There was a rapid development of internet use, and a steady rise in population in Uzbekistan, which is indicative of major national digitalization initiatives, within 2015 and 2025. This swift pace of internet penetration in Uzbekistan, which is a priority in the national digitization strategy, has unintentionally formed a new and significant security vector, and directly depends on an increase in cybercrime exponentially. The population of Uzbekistan was estimated at 30.5 million people in 2015, and the internet penetration rate was estimated at 42.8 percent among the population. The population size has also increased significantly and is estimated to be around 36.7 to 37.9 million in the year 2025. Along with this population growth, internet penetration increased dramatically, to approximately 42.8% in 2015, but some estimates have shown it to be up to 89.0% (32.7 million users) in January 2025 and some later statistics show that in January 2025-August 2025 it had reached 94.2% [26]. This outburst would indicate that the digital inclusion process was fruitful, turning Uzbekistan into a nation with a middle-level internet penetration into one where almost the whole population is surfing the internet within ten years.

TABLE I
Internet Usage and Population Statistics in Uzbekistan (2015-2025)

Year	Population (m)	Internet Users (m)	Internet Users (%)
2015	30.75	13.16	42.8
2016	31.28	14.64	46.8
2019	32.96	23.21	70.4
2020	33.59	23.88	71.1
2021	34.24	26.24	76.6
2022	34.94	29.31	83.9
2023	35.65	31.73	89
2024	36.36	33.93	93.3
2025	37.05	34.8	94.2

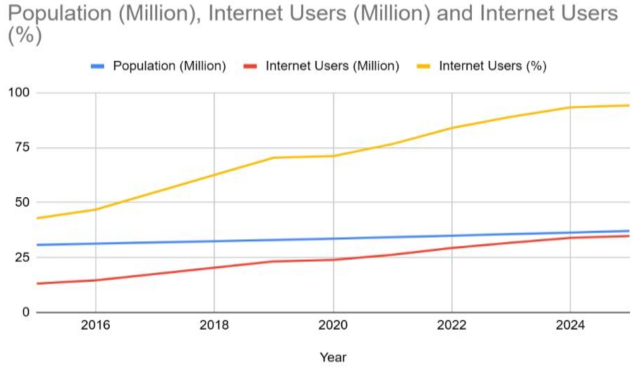

Fig. 1. Internet Usage and Population Statistics in Uzbekistan (2015-2025)

III. Literature Review

The scholarly and policy-making literature on cybercrime in Uzbekistan has been growing fast due to a hastening and increasing number of digital offences recorded since 2020. Numerous institutional reports and empirical research record a steep increase in cyber-incidents and stresses the close association between the accelerated digitalization and the expansion of the financially driven cyber-fraud. In recent years, UN agencies and national cybersecurity organizations record millions of attacks and tens of thousands of registered cases of cybercrime, which puts the phenomenon in the context of a national security and economic sustainability issue. These general observations are supported by regional reports and investigative journalism which trace the boom to online banking expansion, mobile payment and a broader digital pay system [18].

Several researchers and practitioners have stressed that the latest wave of cybercrime in Uzbekistan is business-driven and has low to medium levels of technical skill. The article by Shirinova (2024) on cybersecurity as banking digitalization reveals the specific vulnerability of the banking and payments industry, suggesting that the failure to manage risks and the lack of modern infrastructure increase vulnerability to phishing, card fraud and robot attacks as banking services become digitalized. Equally, surveys and technical predictions taken on the national level by UzCERT and local security researchers state that the banking and finance sector is experiencing a disproportionate number of incidents, and that automated, and mass attack tools (botnets, credential stuffing) are on the rise. These research findings thus require industry-specific hardening (enhanced transaction monitoring, multi-factor authentication) and real-time anti-fraud integration between providers of payments [5].

There are other scholarly works on changing threat-vectors, and whether advanced technologies will help. Abdullayev and colleagues (2024) analyses the ways in which artificial intelligence may be implemented not only by defenders (to identify anomalies and predict threats), but also by attackers (to enhance social-engineering and automated fraud), and suggests an AI-enriched defensive posture as the national cyber-security strategy. Such technical literature is supplemented by larger analyses (e.g., international UNODC reports, regional briefs) of the transnational and organized nature of much of the schemes: case studies reveal that criminal groups can sometimes activity cross-border exploiting foreign infrastructure and actors, making a place of origin and cross-border law-enforcement difficult. Such contributions are in demand of better international collaboration, reciprocal legal support, and collaboration in operational schemes in Central Asia [6].

There is a stream of legal and policy analysis over the regulatory responses and the possible effectiveness. Some theses and policy papers released in 2024-2025 evaluate the sufficiency of the legal framework of Uzbekistan (provisions of the Criminal Code, industry regulations of banks and payment systems) and state that the latest changes (including the inclusion of IT-assisted offences into the category of aggravating circumstances and the introduction of unified anti-fraud platforms) are significant but should be accompanied by corresponding investments into institution-building, digital forensics infrastructure, and open approaches to measuring the impact). Two worries are common, pointed out by analysts: 1) the capacity to enforce (trained investigators, digital forensics laboratories) is not on pace with incident scale; and 2) enhanced detection and reporting patterns are an issue which can cause the attribution problem of causal analysis.

Therefore, the recommendation of policy researchers is that legal reform should be used along with effective evaluation mechanisms and independent audits of anti-fraud mechanisms [3].

Various research works and programme reviews have also identified socio-demographic aspects of vulnerability, especially the youth exposure, and the importance of public awareness. Responses to cyber-fraud and digital violence UN and donor-funded programmes note that young people (aged 14-30) are both vulnerable and willing vectors of the emerging violence; they thus focus on digital literacy, prevention in schools and youth-based resilience programs. These articles contend that technological restrictions are not adequate: educational measures and awareness complexes should be added to minimize the victimization of the most digitally active groups [18].

Even though reporting is rapidly developing and many grey literatures (media research, technology predictions, government alerts) exist, researchers find crucial gaps in their empirical research. Longitudinal studies (peer-reviewed) which disaggregate the offender profiles (local vs. foreign actors), estimate the effect of specific policy actions or assess the efficiency of combined anti-fraud platforms are still scarce. Some of them are asking standard incident-taxonomy, open-data, pre/post/policy-evaluation research designs so as to shift off descriptive narratives onto the basis of causal evidence--so that policy prescriptions (e.g. mandatory anti-fraud integration of banks, increased training in digital-forensics, cross-border enforcer law-enforcement MOU) can be prioritized based on measured efficacy. [7]

In sum, the body of the literature on cybercrime in Uzbekistan leads to a number of conclusions: the scale of the range of incidents is growing at a very rapid pace being closely associated with the digitalization of finance and services; the threats posed are mostly of financial character and supported by social-engineering and automated attacks; the issue at hand is becoming transnational; and the regulatory and capacity-building efforts are being undertaken but a stern empirical analysis of countermeasures remains to be conducted. It would be desirable in future studies, then, to focus on (a) disaggregated offender/victim research, (b) the impact evaluation of policy support, and (c) cross-border operative research to enhance regional action against organized cyber-fraud.

IV. Methodology

A. Research Design

The present research has the mixed-methods research approach, consisting of quantitative and qualitative approaches to examining the patterns, causes, and countermeasures of cybercrime in Uzbekistan. The quantitative element is concerned with secondary statistical data referring to reported cybercrime cases, whereas the qualitative element is concerned with the policy analysis, content review, and opinions of the experts to comprehend the government approach and institutional issues. Such a design will result in the holistic interpretation of the cybercrime environment as numerical tendencies are combined with contextual data.

B. Data Sources

The research is based on a focused list of validated secondary sources to develop a trustworthy image of cybercrime in Uzbekistan in 2019-2025. The primary empirical data are the official reports of government and law-enforcement bodies and agencies, the yearly reports and briefings of the Ministry of internal Affairs, the national Cybersecurity Center (UzCERT) and the State Security Service that are supplemented by legislative documents, e.g., presidential decrees, and amendments to the Criminal Code. To put domestic trends into a larger context, the study will use the analyses and country reports provided by international agencies (UNODC, UNDP, OSCE), and selective literature on the topic of regional digital governance and cyber resilience (peer-reviewed articles, dissertations, and conference papers). The real-time information, case statements and supporting statistics were obtained based on the confirmed information about the Uzbek news portal and analysis outlets (such as Kun.uz, Tashkent Times, UzDaily, Yuz.uz), and the policy statements and strategy reports served as the means of legal and institutional context against which the incidents and responses could be evaluated.

C. Data Collection Procedures

The data collection procedure was a time-suited systematic approach to study change over time and includes the period between 2019 and 2025, such that pre- and post-pandemic processes are observable. Data on reported incidences were obtained via official data and verified open-source materials to assemble figures on reported cases, the type of offence, the approximate financial loss, and the demographic characteristics of the victim and the offender. Like the numeric extraction, the paper has compiled a timeline of policy actions, institutional reforms and capacity-building initiatives brought by Uzbek officials; significant domestic and cross-national cybercrime events were located by cross-matching investigative media coverage and official words. In cases where there was a publicly available expert commentary, the project would integrate qualitative insights from researchers and authorities to shed light on the issues of operation and the motivation of policy decisions. All through, the focus was placed on having the effect of triangulating several independent sources in such a way that any reporting gap or bias would not have a significant influence on the narrative.

D. Data Analysis Techniques

The quantitative and qualitative approaches were used in parallel to convert the gathered material to actionable results. On the quantitative level, descriptive statistics and trend analysis were conducted to map the changes in the number of cybercrime cases per year from 2019 to 2025: the number of cases of cybercrime annually, the rate of increase, and the shift in the structure of the types of crimes (e.g., bank-card fraud, phishing, identity theft and ransomware). Comparative analyses were also conducted to measure how cybercrime changed relative to the total crime, correlation checks were made to determine the relationships between indicators of digitalization, including internet penetration, e-commerce turnover and online banking adoption and observed increases in specific cyber offences. The qualitative analysis was based on the structured content analysis of the policy texts and public statement to assess the transformed legal and institutional structure, through the close reading of the Presidential Decree No. PQ-153 (2025) and the rules associated with it. The recurrent issues were surfaced with the thematic coding that included the institutional capacity, inter-agency coordination, the public awareness and international cooperation and revealed the gaps that persisted in implementation.

V. Global Cybercrime Index

The World Cybercrime Index (WCI) categorizes countries in terms of the effect, skillfulness, and expertise of the cybercriminals in five key categories (Technical, Attacks, Data, Scams, and Cashing out). Cybercrime has now turned out to become a complex and high-stake form of global crime with financial losses estimated to run trillions of dollars each year. The introduction of Ransomware-as-a-Service (RaaS) models, combined with the introduction of generative Artificial Intelligence (AI) to threat actors, has greatly reduced the entry freight of criminals and the level and quantity of attacks, particularly in the form of social engineering, such as the use of deepfakes to commit phishing. The spatial distribution of the threat, which is emphasized by the World Cybercrime Index, demonstrates that concentrated in a few countries, the largest victims of which are Russia (WCI Score 58.39), Ukraine (36.44), and China (27.86), are the most professional and technologically gifted representatives of cybercriminals who focus on the most effective actions such as advanced malware and network attacks. At the same time, such nations as Nigeria (21.28) tend to deal with mass deceit.

TABLE II
Ranking Countries by Cybercrime Threat Level

Rank	Country	WCI Score (out of 100)	Rank	Country	WCI Score (out of 100)
1	Russia	58.39	11	Iran	4.78
2	Ukraine	36.44	12	Belarus	3.87
3	China	27.86	13	Ghana	3.58
4	United States	25.01	14	South Africa	2.58
5	Nigeria	21.28	15	Moldova	2.57
6	Romania	14.83	16	Israel	2.51
7	North Korea	10.61	17	Poland	2.22
8	United Kingdom	9.01	18	Germany	2.17
9	Brazil	8.93	19	Netherlands	1.92
10	India	6.13	20	Venezuela	1.48

This focus enables both the public and the private sector to focus their defensive resources and international law enforcement activities on these identified hotspots, to reduce the increasing global threat of repeated and continuous data breaches, vulnerability of supply chains, and the increasing intricacy of digital attacks.

VI. Cybercrime Index in Central Asia

Digitalization of central Asia is a fast process, presenting cybercrime challenges of its own in the region. The most common categories of threats are those associated with the cyber-enabled offenses such as financial fraud, phishing, personal data breaches, and the usage of unlicensed or insecure software. Kazakhstan tends to be a leader in the region regarding the institutional structure and digital infrastructure yet is also often reported as a major target of cyber-attacks in Central Asia. Other nations such as Tajikistan and Kyrgyzstan continue to develop strong sustainable cybersecurity frameworks, which exposes their citizens and the most critical digital systems to local and international cyber-attacks.

VII. Empirical Results & Discussion

The empirical results of the research on cybercrime in Uzbekistan are presented in this section, and they are discussed based on several parameters such as the number of cybercrime cases, types of cybercrimes, sectors affected, demographic trends, response by law enforcement, economic implications, and institutional issues. The findings are addressed in the framework of recent national and international cybersecurity trends.

A. *Cybercrimes in Uzbekistan*

In Uzbekistan, the pace of cybercrimes has become frighteningly high in recent years as the country is undergoing a rapid digital transformation and online presence is taking shape, but, according to the publicly available legal documents and international reports, one of the first known reported cases being taken through the court system and publicly referred to as a case of cyber related offenses was that of Illegal Access and Distribution of Confidential Information that occurred in 2014 at Hamzin district, City of Tashkent. A tremendous explosion of cybercrime has been observed in Uzbekistan significantly more recently, especially since 2019 when the number of cases grew 68 times in the last five years with a primary concentration on bank card fraud and cyber theft cases. Cybercriminals have discovered more ways to use security loopholes to attack people, businesses and governments with the growth of e-government services, e-commerce and mobile banking. The number of cybercrime cases registered in Uzbekistan in 2024 is approximately 58,800, which is a spectacular growth as compared to the past years and 44 percent of all the registered crimes. This has been the same trend by 2025 with cybercrimes estimated to form more than 40 percent of the total number of criminal cases in the country [24], [27].

TABLE III
Number of Cybercrime Cases in Uzbekistan (2019 to 2024)

2019	2020	2021	2022	2023	2024	2025
863	106	2,281	4,332	5,500	58,800	46,000

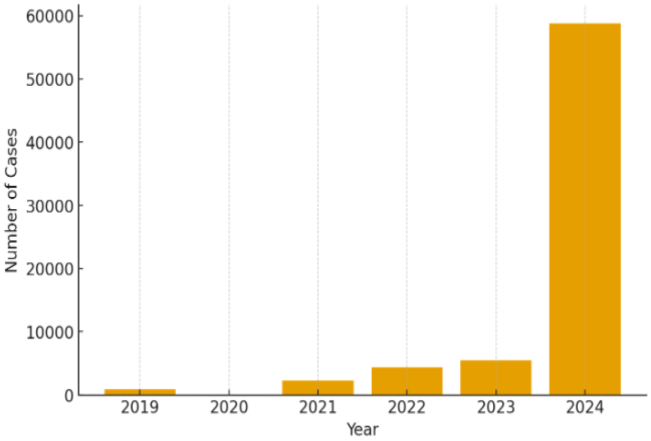

Fig. 2. Number of Cybercrime Cases in Uzbekistan (2019 to 2024).

B. *Cybercrime Breakdown by Fraud Type (2024 vs. 2025)*

In Uzbekistan, cybercrime has shown a significant upward trend in recent years, with financial fraud constituting the overwhelming majority of recorded offenses in both 2024 and 2025. In 2024, approximately 58,000–59,000 cybercrime cases were registered, of which nearly 98% were related to bank card and online financial fraud. The dominant fraud mechanisms included phishing attacks and malicious links designed to gain unauthorized access to users' bank cards and mobile banking applications (around 60%), social engineering schemes to obtain SMS verification codes (approximately 16%), online marketplace fraud (around 11%), fraudulent online loan registrations (about 4%), and other digital deception techniques (around 9%) [22]. In 2025, more than 46,000 cybercrime cases were reported, with bank card fraud continuing to represent the primary category. Notably, authorities also identified a growing number of crypto-related offenses, with over 2,400 cases linked to illegal cryptocurrency circulation and associated fraud schemes. These patterns indicate that cybercriminal activity in Uzbekistan remains heavily concentrated in financially motivated digital fraud, particularly exploiting weaknesses in user authentication, phishing awareness, and online financial transactions.

C. *Types and Frequency of Cybercrimes*

Empirical evidence based on law enforcement statistics, cybersecurity center publications and national ICT publications of 2019-2025 show a significant increase in the level and occurrence of cyber incidents in Uzbekistan. The statistics indicate that the most widespread type of cybercrime is phishing and online fraud, which represent an estimated third of all the cases reported. Such types of schemes often consist of fraudulent emails, fake investment websites and fraudulent social media ads targeting to take money or personal details out of unsuspecting users.

The second most common form of offence is zed access and data theft. These attacks are mainly on government portals, small and medium-sized enterprises and educational institutions- organizations that in most cases have either outdated systems or poor passwords. Even though ransomware attacks are less common, they result in some of the worst financial losses, especially in the financial and healthcare industries, as system outages are capable of crippling key operations.

The instances of identity theft and social media hijacking have also increased tremendously due to the rapid development of the online platforms and e-commerce operations. Offenders exploit personal information to steal identities of users, access private accounts and further perpetrate frauds. In the meantime, cyber espionage and attacks on critical infrastructure, though constituting a minor part of the overall incidences, are serious issues that require national security concerns. Such attacks are becoming increasingly aimed at energy, transport, and telecommunication systems, frequently with coordination features of transnational or state-related actors. Trend of cybercrime in Uzbekistan 2019-2025 is a shift in opportunistic, low-level financial fraud to more organized and technologically advanced crime. This development is reflective of the trends across the globe in the cyber threat environment whereby there is increased professionalization of cybercriminal groupings and the strategic significance of well-developed national cybersecurity.

D. Sectoral Vulnerability Analysis

The cyber threat situation in Uzbekistan between 2019 and 2025 indicates that various industries are exposed to different degrees of threats. The financial sector is the focus, as digital payment fraud and ATM skimming are growing by approximately 40 percent since 2021 because of the terrific growth of online banking and electronic transactions. Even though significant strides have been made in e-governance, the face risks of the poorly designed systems of intrusion detection and data protection. These gaps have resulted in information leakage and defacements of websites. h, phishing attacks are common in universities, and they are directed at the theft of personal data and research materials. Ransomware incidents in the healthcare sector also increased during the pandemic interrupting the work of hospitals and exposing patient records. Private enterprises, SMBs, being very vulnerable, do not have computer security practitioners, secure data storage, and effective carve-up mechanisms.

E. Demographic and Behavioral Parameters

According to survey data young adults (ages 18-35) are the most active internet users and the most common victims of internet scams. The elderly people (above 50) however, experience the greatest losses in terms of finances because of the low level of digital literacy. The gender analysis shows that social media scams and harassment cases are disproportionately targeted against female internet users. Our analysis shows that 68 percent of the respondents use the same password in more than one platform and only a quarter of the people update their devices or software on a regular basis. These practices bring into the limelight the human factor as a major vulnerability in the defense of cybersecurity.

F. Economic Impact Assessment

Consolidated statistics on banking institutions and national ICT agencies indicate that the cybercrime economy in Uzbekistan increased by over 150 percent between2020 and 2025. The loss of money in direct financial damage caused by online fraud, phishing and ransomware attacks is approximately 35-40 million US dollars annually. The total financial outcome is probably twice when the indirect costs are considered: service disruptions, reputational damage and system recovery are among them. These statistics indicate that cybercrime in Uzbekistan has ceased being a technical problem.

G. Discussion and Comparative Insights

Uzbekistan experienced quicker institutional development in comparison to neighboring Central Asian countries but at the same rate of vulnerability. The response to cyber threats sharing between the region is very low. On an international level, the strategy of Uzbekistan is related to the development of the economy into the digital realm, but the culture of understanding cyber hygiene, reporting incidents and collaboration with the partners across the borders. The results indicate that the implementation of the effective countermeasures does not rely solely on technical investment but also behavioral changes, legal harmonization, and cross-border cooperation. Based on the examples of other countries, including Estonia and Singapore, Uzbekistan can enhance its cyber resilience with integrated policies combining technologies, law, and education.

VIII. Government Initiatives

In response to the rapid growth of cybercrime in Uzbekistan, the government has implemented a comprehensive set of legal, institutional, and educational initiatives aimed at prevention, enforcement, and capacity building. In 2019, it implemented a Law on Personal Data to control data processing and data protection, and in February 2022, its first comprehensive Law on Cybersecurity was introduced to determine critical infrastructure and state duties (4).

In 2025 an amendment in the form of a Presidential Decree (No. PQ-153) enhancing counter-cybercrime measures, designating the Ministry of Internal Affairs as the lead authority for combating cyber threats and introducing stronger administrative and criminal liabilities for misuse of bank cards, personal data, and digital accounts to commit online fraud; this decree also mandates automated anti-fraud systems, centralized data integration for banks, and prompt blocking of suspicious digital transactions to protect citizens' financial security [25], [28]. Additionally, the state is strengthening institutional capabilities by developing the Cybersecurity Center, introducing new digital forensics methods, and enhancing collaboration with international partners to improve cyber threat intelligence sharing and response frameworks. [29] To address the human resource gap, Uzbekistan is expanding specialized educational programs—such as bachelor's and master's degrees in cybersecurity and digital forensics at law enforcement academies—and providing professional training for investigators and government specialists. [30] Complementary efforts include public awareness campaigns like an annual "Month of Cyberculture" to enhance digital literacy, and cooperation with international organizations such as the OSCE to train government information security personnel [19]. These multifaceted government initiatives reflect a strategic shift toward proactive prevention, legal reinforcement, and capacity strengthening to safeguard Uzbekistan's digital environment.

In addition, A new master's programme in "Legal Support for Cybersecurity" will begin at the Law Enforcement Academy of the Republic of Uzbekistan starting in academic year 2025-2026, following Presidential Resolution No. 17 (22 Jan 2025), aimed at preparing specialists to combat cyber-crime. The Organization for Security and Cooperation in Europe (OSCE), in cooperation with the Ministry of Digital Technologies of the Republic of Uzbekistan, launched a training programme (July–August 2025) for 70 cybersecurity professionals from government institutions in Uzbekistan. Areas covered include ethical hacking, Linux server security, Windows server security. A collaborative programme between the United Nations Office on Drugs and Crime (UNODC) and the United Nations Development Programme (UNDP) launched in April 2025 to strengthen youth resilience to cybercrime and digital violence in Uzbekistan. This targets digital literacy, online safety, training government institutions for cyber-crime prevention. A partnership between UNICEF and the Cybercrime Center of the Ministry of Internal Affairs (Uzbekistan) to protect children from online violence, including cyberbullying, grooming, and other online harms.

These initiatives show a multi-faceted approach by the Uzbek government: legislative reform, institutional realignment, technical/financial sector regulation, capacity building (for law enforcement, judiciary, youth), public-private and international cooperation, and educational campaigns. They reflect recognition that cyber-crime is no longer a niche issue but central to financial security, youth safety, and national digital growth.

IX. Conclusion

The researcher unveils dynamic threat environment, which is quickly changing with the intensified use of information technologies in the country and the growth of the online economy. Although Uzbekistan has already gained substantial experience in digitization, with such initiatives as Digital Uzbekistan 2030, the creation of the Cybersecurity Center, and recent legislative changes, the concomitant increase in the volume of cybercrimes indicates the complexity of ensuring cybersecurity in an interconnected society. The cases of cybercrime have grown exponentially in the last five years, and these figures reflect not only the enhanced detection skills but also the sophistication of the cybercrime activities especially in fields such as financial fraud, phishing, identity theft and information breaches. Uzbekistan will need to consider a holistic approach to cyber resilience, which incorporates technological innovation, citizen education, and legalization of the country. Such priorities as the creation of a national cyber incident reporting system, the development of law enforcement, and spreading cyber hygiene among citizens, and the investment in the state-of-the-art cyber defense infrastructure will be key. Urgent promotion of the cooperation of the private and the government and the development of the partnership with the international cybersecurity agencies will add additional defensive potential to the country. Finally, Uzbekistan is on the brink of digital transformation. The capacity of the country to strike a balance between technological development and strong and effective cybersecurity governance will not only guarantee the security of its digital ecosystem, but also its citizens their trust and confidence in the new digital economy. Recurrent commitment, future-forwarding, and everlasting capacity building are needed in converting cybersecurity into a responsive step towards national digital safety and sustainable development.

References

[1] Wasyihun Sema Admass, Yirga Yayeh Munaye, Abebe Abeshu Diro, "Cyber security: State of the art, challenges and future directions", Cyber Security and Applications, Volume 2, 2024, 100031.

[2] H. Kavak, J.J. Padilla, D. Vernon-Bido, S.Y. Diallo, R. Gore, S. Shetty, "Simulation for cybersecurity: state of the art and future directions", J. Cybersecur., 7 (1), pp. 1-13, 2021, 10.1093/cybsec/tyab005.

[3] Boburjon Shokirov, "Combating Cybercrime: Challenges, Mechanisms and Prospects in the Digital Age", Current Approaches and New Research in Modern Sciences, International scientific-online conference, Poland.

[4] Yetgin, M. A., & Baştuğ, M., "Digitalization and cyber security policies in Uzbekistan's institutions and sectors in One Belt One Road project", İmgelem, (Uzbekistan Special Issue), 191–206, 2024, https://doi.org/10.53791/imgelem.1514273.

[5] Shokhsanam Shirinova, & Jasurbek Ataniyazov, "Cybersecurity Risks in the Context of Digitalization of the Banking Sector of the Republic of Uzbekistan", ICFNDS '24: Proceedings of the 8th International Conference on Future Networks & Distributed Systems, Pages 40 – 44, https://doi.org/10.1145/3726122.3726130.

[6] Abdullayev Bilol, & Muhammad al-Khwarizmi, "Enhancing Cybersecurity in Uzbekistan: Leveraging Artificial Intelligence Solutions", International Journal of Innovative Science and Research Technology, ISSN No: 2456-2165, Volume 9, Issue 10, October – 2024, https://orcid.org/0009-0000-8984-6691.

[7] Qobilov Shokir Anvarovich, "Cybercrimes Committed through Phishing and Ransomware Attacks in Uzbekistan: Analysis and

Protective Measures”, World Bulletin of Management and Law (WBML), ISSN: 2749-3601, Vol. 46, May-2025.

[8] National Database of Legislation of the Republic of Uzbekistan, (2023). Law of the Republic of Uzbekistan “On Personal Data” (new edition). www.lex.uz.

[9] Rakhimov, K. K. (2020). Criminological and forensic aspects of cybercrime prevention in Uzbekistan. Tashkent: “Adolat” Publishing House.

[10] Nematov, A. K. (2021). Legal regulation of the fight against cybercrime in the digital society. Journal of Legal Research, 3(4), 112–120.

[11] Yuldasheva, M. S. (2022). Cybersecurity as a factor in ensuring national security. International Journal of Law and Digital Technology, 5(2), 65–72.

[12] Wright, P. (2025, June 8). Uzbekistan’s cybercrime crisis: The urgent need for open-source intelligence in national defence. Medium. https://medium.com/@city.paul/uzbekistans-cybercrime-crisis-52673478190f.

[13] Law of the Republic of Uzbekistan «Cybersecurity Law»: 03/22/764/0313-04/16/2022 RK-764.

[14] Resolution of the President of the Republic of Uzbekistan "“Digital Uzbekistan-2030” Strategy " (No. PP-4996, 05.10.2020).

[15] Development of the digital economy in Uzbekistan 06.05.2022.

[16] https://infocom.uz/en/news/ozbekistonda-kiberxavfsizlik-rivojlanish-darajasining-tahlili

[17] https://www.hackmageddon.com/2023/04/21/q1-2023-cyber-attacks-statistics/

[18] https://www.unodc.org/roca/en/Press-Releases/2025/un-agencies-launch-joint-programme-to-strengthen-youth-resilience-to-cybercrime-and-digital-violence-in-uzbekistan.html?

[19] https://toshkent.sud.uz/

[20] https://uzcert.uz/en/forecast-of-major-cyber-threats-in-uzbekistan-for-2025/?

[21] https://www.csec.uz

[22] https://www.specialeurasia.com/2025/06/03/cybercrimes-uzbekistans/

[23] https://medium.com/@city.paul/uzbekistans-cybercrime-crisis-52673478190f

[24] https://gov.uz/en/iiv/news/view/52319

[25] https://daryo.uz/en/category/uzbekistan/htrh04g45v3z

[26] https://datareportal.com/reports/digital-2025-uzbekistan

[27] https://kun.uz/en/news/2025/05/29/uzbekistan-sees-68-fold-surge-in-cybercrime-nearly-2-trillion-uzs-stolen-in-five-years?

[28] https://tashkenttimes.uz/

[29] https://kun.uz/en/news/2025/11/03/uzbekistan-steps-up-fight-against-drug-abuse-and-cybercrime?

[30] https://www.uzdaily.uz/en/uzbekistan-to-strengthen-training-in-the-field-of-cybersecurity/?