The OSCAR PUBLISHING Services
International Journal of Law And Criminology

VOLUME Vol.06 Issue05 2026
PAGE NO. 42-47
DOI 10.37547/ijlc/Volume06Issue05-07

Cybersecurity In The Republic Of Uzbekistan: Legal Framework, Emerging Threats, And Prospects For Reform

Abdushukurova Nozimabonu Abdullo kizi
Lecturer at the Mirzo Ulugbek National University of Uzbekistan

Received: 30 March 2026; **Accepted:** 25 April 2026; **Published:** 16 May 2026

Abstract: The rapid expansion of digital infrastructure in Uzbekistan has been accompanied by a dramatic surge in cyber threats and criminal activity in cyberspace. This article examines the cybersecurity legal framework of the Republic of Uzbekistan, focusing on the landmark Law No. ZRU-764 'On Cybersecurity' (2022) and its interaction with pre-existing legislation, including the Criminal Code, the Law on Personal Data (2019), and the Digital Uzbekistan 2030 Strategy. Drawing on official statistical data, legislative analysis, and comparative review of international standards, the study assesses whether the existing legal regime is adequate to address the scale and sophistication of contemporary cyber threats. Key findings indicate that while Uzbekistan has made significant legislative strides, critical gaps remain in enforcement mechanisms, data protection harmonisation, and institutional capacity. The article concludes with reform recommendations aligned with international best practices and the Budapest Convention on Cybercrime.

Keywords: Cybersecurity law; Uzbekistan; digital governance; cybercrime; Critical Information Infrastructure; data protection; Digital Uzbekistan 2030; Budapest Convention.

Introduction: The digitalisation of economies and public services has profoundly altered the threat landscape facing modern states. Uzbekistan, a lower-middle-income country of approximately 37 million people in Central Asia, has pursued an ambitious programme of digital transformation encapsulated in its 'Digital Uzbekistan 2030' Strategy, approved by presidential decree. The strategy envisions Uzbekistan ranking among the top 30 countries in the United Nations E-Government Development Index by 2030 - an ambition the country is actively pursuing, having climbed to 63rd place in the 2024 UN E-Government Survey (up from 69th in 2022) and entering the 'very high' EGDI category for the first time (Global BIM Network, 2024).

Yet rapid digitalisation has a shadow side. Between 2019 and 2024, cybercrime in Uzbekistan increased by over 6,700 percent, and by 2024 cyber-related offences accounted for 44.4 percent of all registered criminal cases (Special Eurasia, 2025). The Center for Cyber Security of Uzbekistan recorded 11.2 million cyberattack attempts against national web resources in 2023 alone, with attack traffic originating predominantly from the Netherlands, the United States, Russia, Germany, India, and China (Business Upturn, 2024). In the first five months of 2024 alone, more than 6.6 million attacks were recorded, signalling an accelerating trajectory (Daryo, 2024).

Despite these developments, Uzbekistan had no dedicated cybersecurity statute until April 15, 2022, when the Law of the Republic of Uzbekistan No. ZRU-764 'On Cybersecurity' entered the legal order, coming into force on July 17, 2022 (Dentons, 2022). The enactment of this landmark legislation prompted a series of secondary regulations, creating a nascent but still evolving legal infrastructure. Scholarly attention to this framework, however, remains sparse in English-language literature, and the adequacy of the framework has not been systematically evaluated against the scale of documented threats.

This article seeks to fill that gap. Its central research question is: Does the current cybersecurity legal framework of Uzbekistan adequately address the nature, scale, and complexity of contemporary cyber threats facing the country? Subsidiary questions concern the institutional architecture created by the 2022 Law, the adequacy of criminal law provisions, the coherence of data protection regulation, and the extent of international legal alignment.

The article proceeds as follows. Section 2 describes the methodology. Section 3 provides a contextual overview of the digital environment and threat landscape. Section 4 analyses the primary legal instruments. Section 5 identifies critical gaps and limitations. Section 6 discusses findings in comparative perspective. Section 7 concludes with reform recommendations.

Methodology

This article employs a doctrinal and comparative legal research methodology. The primary method is legislative analysis: each principal legal instrument is examined for its structure, definitional scope, institutional assignments, and enforcement mechanisms. Primary sources include the full text of Law No. ZRU-764 (2022), the Law on Personal Data No. ZRU-547 (2019), the Law on Informatisation No. 560-II (2003), the Criminal Code of the Republic of Uzbekistan (1994, as amended), and presidential decrees implementing the Digital Uzbekistan 2030 Strategy.

The comparative dimension draws on the Budapest Convention on Cybercrime (Council of Europe, 2001), the European Union's General Data Protection Regulation (GDPR, 2016/679), and the United Nations Guide to Developing a National Cybersecurity Strategy (UN, 2021), which together constitute internationally recognised benchmarks. Published secondary sources - peer-reviewed articles, official reports, and authoritative legal commentaries - supplement the primary analysis.

Quantitative data on cyberattack volumes and cybercrime rates are drawn from official publications of Uzbekistan's Center for Cyber Security and third-party analytical reports. All legal translations from Uzbek and Russian are the author's own unless otherwise noted. This study is limited to the domestic legal framework and does not purport to provide a full technical security audit.

RESULTS: DIGITAL ENVIRONMENT AND THREAT LANDSCAPE IN UZBEKISTAN

Uzbekistan's commitment to digital transformation is reflected in sustained public investment. The Digital Uzbekistan 2030 Strategy contemplates the attraction of approximately USD 2.5 billion for digital infrastructure development and the implementation of over 280 digitisation projects across sectors and regions (Government of Uzbekistan, 2024). As of the first quarter of 2026, the volume of communication and informatisation services reached 22,827.9 billion soums - a figure illustrating the economic centrality of the digital sector (Ministry of Digital Technologies, 2026). Internet penetration and mobile banking adoption have expanded rapidly, creating new opportunities but also new attack surfaces for criminal actors.

The government has aligned digital strategy with e-government expansion. The 2024 UN E-Government Survey placed Uzbekistan 63rd globally, its highest ranking to date and the first time it entered the 'very high' EGDI category (Global BIM Network, 2024). This progress, while commendable, creates systemic cybersecurity dependencies: the more critical services migrate online, the more consequential any cyber breach becomes for public administration and citizens alike.

The threat data from Uzbekistan is striking in its magnitude and growth rate. According to the Center for Cyber Security, 11.2 million cyberattack attempts were recorded against Uzbekistani web resources during 2023, with the Netherlands accounting for over 759,000 source-IP attacks - an unexpected geographic concentration that illustrates the transnational character of cyber threats (Business Upturn, 2024). In the first five months of 2024, 6.6 million attacks were registered, suggesting the annualised rate substantially exceeded the 2023 figure (Daryo, 2024).

At the criminal law level, cybercrime's share of total registered crime rose from a negligible baseline in 2019 to 44.4 percent of all criminal cases in 2024 - representing a documented increase of over 6,700 percent in five years (Special Eurasia, 2025). The dominant attack typologies include malicious software and phishing links (60 percent of incidents), social-engineering attacks exploiting SMS authentication codes (16 percent), fraudulent loan origination through digital identity misuse (4 percent), and commercial platform fraud (11 percent) (Special Eurasia, 2025). Banking card fraud constitutes the largest single subcategory, reflecting both the rapid growth of digital financial services and insufficient consumer-level cyber literacy.

The cybersecurity market is correspondingly expanding. Statista projects Uzbekistan's cybersecurity market revenue will grow at a compound annual rate of 11.33 percent between 2025 and 2030, reaching USD 150.29 million by 2030 (Statista, 2025). This growth, while positive for sector maturation, also signals that

current defensive capacity lags behind threat expansion.

ANALYSIS: THE CYBERSECURITY LEGAL FRAMEWORK

The Law of the Republic of Uzbekistan No. ZRU-764, adopted on April 15, 2022 and entering into force on July 17, 2022, is the country's first comprehensive statute dedicated exclusively to cybersecurity (CIS Legislation, 2022). Consisting of 40 articles, the Law introduces a set of foundational legal concepts - cybercrime, cyberspace, cyber threat, cybersecurity, cyber defence, cyberattack, and Critical Information Infrastructure (CII) - that were previously absent from or inconsistently defined across Uzbekistani legislation (GRATA Net, 2022).

Institutionally, the Law vests the State Security Service of the Republic of Uzbekistan (SSS) as the authorised state body in the field of cybersecurity, while reserving to the President the determination of unified state cybersecurity policy (Black Swan Law, 2023). The SSS is empowered to develop regulatory legal acts and government programmes, conduct operational-search activities and pre-investigation checks in connection with cybersecurity incidents, and take enforcement action. This concentration of cybersecurity authority in an intelligence agency rather than a civilian body has attracted academic commentary on the potential tension between security objectives and civil liberties protections (Nematullayev, 2022).

The Law prescribes a structured incident-response framework. Cybersecurity subjects - defined to include both public and private operators of information systems - are required to take measures in the following forms: preventing vulnerabilities and errors in software and devices; destroying malicious programmes and limiting their distribution; implementing technical and organisational safeguards; and notifying the authorised body of incidents (GRATA Net, 2022). CII operators bear heightened obligations, including mandatory incident reporting and compliance with government-prescribed security standards.

Despite these advances, several limitations of Law No. ZRU-764 have been identified in legal commentary. Business Upturn (2024) noted that, at the time of enactment, the Law had not yet fully consolidated provisions scattered across pre-existing telecommunications and internet security legislation. The Law also defers many implementation details to secondary normative acts, creating a gap between formal enactment and practical enforcement that persists where those secondary instruments are absent or incomplete.

Law No. ZRU-764 operates within a broader legislative ecosystem. The Law on Informatisation No. 560-II (2003) established the general framework for information systems regulation and contains foundational provisions on information security. The Law on Principles and Guarantees of Freedom of Information No. 439-II (2002) addresses the public's right of access to information. The Law on Personal Data No. ZRU-547 (2019) governs the collection, processing, and protection of personal data and is supplemented by Cabinet of Ministers Resolution No. 570 (October 5, 2022), which establishes differentiated protection levels based on threat categorisation, including requirements for physical security, role-based access control, encryption, and internal auditing (Legal 500, 2025; DLA Piper, 2025).

At the standards level, Uzbekistan has adopted national versions of the ISO/IEC 27000 series. O'zDSt ISO/IEC 27002:2024 provides guidance on information security controls, while O'zDSt ISO/IEC 27005:2024 addresses risk assessment and management - demonstrating a commitment to aligning domestic practice with globally recognised frameworks (Legal 500, 2025).

Cybercrime criminalisation in Uzbekistan is grounded in the Criminal Code of the Republic of Uzbekistan (1994, as amended). The Code proscribes a range of cyber-enabled offences including illegal access to computer systems, computer fraud, digital identity theft, and related digital harassment (Law Gratis, 2025). These provisions antedate the 2022 Law and have been periodically amended to extend their scope.

However, a review of public reporting on criminal liability reform reveals ongoing acknowledged gaps. In 2022, the government's 'Roadmap' for the Development Strategy 2022–2026 explicitly identified a planned review of criminal liability for cybercrime and the creation of a cybercrime prevention system (Kun.uz, 2022). The Presidential Decree No. 38 of March 10, 2026, establishing the Cybersecurity Strategy for 2026–2030, further signals the government's recognition that the existing criminal law architecture requires strengthening to match contemporary threat profiles (Nurilla, 2026).

Uzbekistan's international legal obligations in the cybersecurity sphere are primarily anchored in the three United Nations drug control conventions and, in the cyber context, in its membership of the Shanghai Cooperation Organisation (SCO), which promotes regional cooperation on cybersecurity and digital governance (Law Gratis, 2025). Additionally, Uzbekistan is reported to be a signatory to the Budapest Convention on Cybercrime - the most substantive multilateral instrument for harmonising cybercrime law and enabling cross-border law

enforcement cooperation (Law Gratis, 2025; Council of Europe, 2020).

The Budapest Convention's Article 2–10 requires criminalisation of illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, child pornography, and copyright-related offences. Aligning Uzbekistan's Criminal Code fully with these categories remains a policy objective cited in the 2026–2030 Cybersecurity Strategy.

Discussion: Critical Gaps And Limitations

Notwithstanding the legislative progress described above, the analysis reveals four categories of critical gap.

First, enforcement capacity remains limited. The dramatic statistical increase in cybercrime - a 6,700-percent rise over five years - substantially outpaces the growth of institutional response capacity. Law enforcement agencies have reported insufficient technical expertise, outdated forensic infrastructure, and limited inter-agency coordination (Special Eurasia, 2025). The assignment of cybersecurity authority primarily to the SSS, an intelligence-oriented agency, creates structural questions about whether cybercrime prosecution and civilian cyber incident response receive adequate specialised attention.

Second, data protection coherence requires strengthening. The Law on Personal Data (2019) was enacted before the 2022 Cybersecurity Law, and the two instruments were not drafted with full mutual coherence. The Cabinet of Ministers Resolution No. 570 (2022) and the Ministry of Justice Orders No. 3477 and 3478 (2023) have subsequently elaborated the personal data framework, but sector-specific regulations in finance, health, and telecommunications remain fragmented (DLA Piper, 2025). The absence of an independent data protection supervisory authority - analogous to the supervisory bodies required under GDPR Article 51 - is a notable structural gap by international standards.

Third, cyber literacy and private-sector compliance remain uneven. The dominant attack vector - malicious software and phishing (60 percent of incidents) - is primarily defeated not by law but by informed user behaviour and organisational security culture (Special Eurasia, 2025). The 2022 Law imposes compliance obligations on CII operators but provides limited guidance for small and medium enterprises (SMEs), which constitute the majority of Uzbekistan's private sector. The result is an asymmetric compliance burden that leaves a large attack surface inadequately governed.

Fourth, the legal treatment of emerging technologies remains nascent. Artificial intelligence, blockchain-based transactions, and cryptocurrency platforms create novel threat vectors and regulatory challenges. The Presidential Decree on the AI Development Strategy to 2030 (October 2024), which allocates USD 50 million for AI infrastructure and targets the training of one million specialists (Government of Uzbekistan, 2024), is not accompanied by a commensurate legal framework addressing AI-enabled cyberattacks, algorithmic accountability, or cryptocurrency-related cybercrime.

Comparative Perspective

Uzbekistan's trajectory is broadly comparable to that of other middle-income post-Soviet economies that enacted first-generation cybersecurity frameworks in the early 2020s. Kazakhstan adopted a comprehensive cybersecurity law in 2017 and has since developed a more elaborate institutional architecture, including a dedicated state cybersecurity committee separate from its national security apparatus. Georgia's cybersecurity framework, developed with Council of Europe technical assistance under the Budapest Convention, provides a civil-society-inclusive model of cyber governance that Uzbekistan may find instructive.

At a broader level, the UN Guide to Developing a National Cybersecurity Strategy (2021) identifies five core functions of an effective national cybersecurity strategy: identify, protect, detect, respond, and recover. Uzbekistan's 2022 Law addresses the protect and detect functions in reasonable detail, but the identify (comprehensive asset and risk mapping), respond (clear incident command structures), and recover (business continuity and resilience frameworks) functions are less well developed in statute.

The GDPR framework, while not directly applicable in Uzbekistan, has influenced corporate compliance programmes in Uzbek companies operating in cross-border contexts and serves as a benchmark for data protection reform (Legal 500, 2025). A move toward an independent data protection supervisory authority, combined with a harmonised enforcement regime, would substantially close the gap between Uzbekistani and European standards.

Conclusion And Recommendations

This article has demonstrated that Uzbekistan's cybersecurity legal framework has advanced substantially since the enactment of Law No. ZRU-764 in 2022, yet remains insufficient to address the scale and sophistication of the cyber threats the country faces. The 6,700-percent increase in cybercrime between 2019 and 2024, the 11.2 million cyberattack

attempts recorded in 2023, and the dominance of social-engineering attack vectors together indicate systemic vulnerabilities that legal reform alone cannot resolve - but which coherent legal frameworks can meaningfully mitigate.

On the basis of this analysis, the following recommendations are proposed. First, Uzbekistan should strengthen institutional architecture by establishing a civilian National Cybersecurity Agency with a mandate distinct from intelligence functions, to coordinate incident response, public-private partnerships, and international cooperation. Second, the Criminal Code should be comprehensively reviewed and updated to achieve full alignment with all criminalisation obligations under the Budapest Convention, including clear provisions on AI-enabled and cryptocurrency-related cybercrime. Third, an independent Personal Data Protection Authority should be established with investigative and enforcement powers, removing personal data oversight from ministry-level administration. Fourth, a national cybersecurity awareness programme should be mandated and funded, targeting both individual users and SMEs, given that the predominant attack vectors (phishing, social engineering) are primarily countered by behaviour rather than legislation. Fifth, the legal framework governing AI, blockchain, and virtual assets should be developed proactively, in coordination with the AI Strategy (2024) and the Cybersecurity Strategy for 2026–2030.

These reforms would position Uzbekistan's cybersecurity governance in alignment with internationally recognised best practices and support the broader ambitions of the Digital Uzbekistan 2030 Strategy. As digital transformation accelerates, the adequacy of the legal framework will increasingly determine whether that transformation delivers its promised developmental benefits or becomes a vector for insecurity and harm.

References

1. Black Swan Law. (2023, February 27). Uzbekistan Law 'On Cybersecurity'. BSC Law Firm. https://blackswan.law/law-on-cybersecurity/
2. Business Upturn. (2024, February 14). Uzbekistan battled 11 million cyberattacks in 2023. https://www.businessupturn.com/technology/cyber-security/uzbekistan-battled-11-million-cyberattacks-in-2023/
3. CIS Legislation. (2022, April 15). Law of the Republic of Uzbekistan 'About Cyber Security' No. ZRU-764. https://cis-legislation.com/document.fwx?rgn=139485
4. Council of Europe. (2001). Convention on Cybercrime (Budapest Convention), ETS No. 185. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
5. Council of Europe. (2020, May 13). The Budapest Convention on Cybercrime: Benefits and impact in practice. Cybercrime Convention Committee (T-CY). https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac
6. Daryo. (2024, August 27). Uzbekistan's cybersecurity challenge: Navigating 25-fold rise in attacks. https://new.daryo.uz/en/category/uzbekistan/pwrhtg4d0xjf
7. Dentons. (2022, April 22). Uzbekistan adopts cybersecurity law. https://www.dentons.com/en/insights/articles/2022/april/22/uzbekistan-adopts-cybersecurity-law
8. DLA Piper. (2025). Data protection laws of the world: Uzbekistan. https://www.dlapiperdataprotection.com/index.html?t=law&c=UZ
9. Global BIM Network. (2024). Digital Uzbekistan 2030 strategy and e-government development. https://globalbim.org/info-collection/digital-uzbekistan-2030-strategy-and-e-government-development/
10. Government of Uzbekistan. (2024). Digital technologies and transport: Digital Uzbekistan 2030 Strategy. https://gov.uz/en/activity_page/digital_technology
11. GRATA Net. (2022, May 19). Uzbekistan adopts Cybersecurity Law. https://gratanet.com/news/uzbekistan-adopts-cybersecurity-law
12. Kun.uz. (2022, January 7). Uzbekistan to review criminal liability for cybercrime. https://kun.uz/en/news/2022/01/07/uzbekistan-to-review-criminal-liability-for-cybercrime
13. Law Gratis. (2025, April 9). Cyber law at Uzbekistan. https://www.lawgratis.com/blog-detail/cyber-law-at-uzbekistan-1
14. Legal 500. (2025, August 7). Personal data compliance in Uzbekistan. https://www.legal500.com/developments/thought-leadership/personal-data-compliance-in-uzbekistan/
15. Lex.uz. (2022). Law of the Republic of Uzbekistan No. ZRU-764 'On Cybersecurity', April 15, 2022. https://lex.uz/en/docs/6997403

16. Lex.uz. (2019). Law of the Republic of Uzbekistan No. ZRU-547 'On Personal Data', July 2, 2019. https://lex.uz/docs/-4378782
17. Nematullayev, A. U. (2022). The issue of ensuring the cybersecurity of the Republic of Uzbekistan in the process of implementing the Strategy 'Digital Uzbekistan 2030'. International Journal of Business and Digital Economy, 3(1). https://inter-publishing.com/index.php/ijbde/article/view/2164
18. Nurilla, A. (2026, March 17). Uzbekistan adopts national cybersecurity strategy to 2030. https://www.nurilla.com/insights/uzbekistan-cybersecurity-strategy-2030.html
19. Special Eurasia. (2025, June 3). Rising cybercrime alarms Uzbekistan's national security. https://www.specialeurasia.com/2025/06/03/cybercrimes-uzbekistans/
20. Statista. (2025). Cybersecurity — Uzbekistan: Market forecast. https://www.statista.com/outlook/tmo/cybersecurity/uzbekistan
21. United Nations. (2021). Guide to developing a national cybersecurity strategy. UN Office of Counter-Terrorism. https://www.un.org/counterterrorism/
22. USAID. (2022, January). Uzbekistan digital ecosystem country assessment (DECA). https://www.usaid.gov/sites/default/files/2022-05/USAID_UzbekistanDECA.pdf