Asian Journal of Criminal Justice and Forensic Studies

Vol. 1, No. 1. 2025

Journal homepage: https://asianjustice.kz/

UDC 341.231:34

Article's History:
Received: 09.06.2025; Revised: 07.11.2025; Accepted: 16.12.2025

Cybersecurity law in Kazakhstan: A comparative analysis with East Asian practices

Gulnoza Ismailova*
University of World Economy and Diplomacy
100007, 54 Mustakillik Ave., Tashkent, Uzbekistan
https://orcid.org/0000-0002-2244-0299

Nargiza Kadirova
University of World Economy and Diplomacy
100007, 54 Mustakillik Ave., Tashkent, Uzbekistan
https://orcid.org/0009-0009-6698-7219

Abstract. The study aimed to identify avenues for modernising the national cybersecurity system of the Republic of Kazakhstan through a comprehensive assessment of its effectiveness and an examination of advanced practices implemented in East Asian states. The legal analysis revealed a fragmented Kazakhstani cybersecurity framework characterised by the absence of a single codified act and by the proliferation of regulatory documents of varying legal force. The empirical assessment demonstrated a sustained rise in cybersecurity incidents in Kazakhstan, with an average annual growth rate of 14.5% between 2019 and 2024, reaching more than 41,000 cases in 2024. The number of recorded cybercrimes increased thirty-six-fold, from 589 cases in 2018 to 21,479 in 2021. The study identified low enforcement effectiveness, with only 36% of registered cases reaching judicial proceedings. Financial losses incurred by citizens as a result of digital fraud exceeded 17.5 billion tenge in 2023. A correlation analysis of the Worldwide Governance Indicators – specifically rule of law, control of corruption, regulatory quality, and political stability – with cybercrime metrics, including the number of registered cybercrimes and the case-clearance rate, identified a statistically significant negative association ($r = -0.67$, $p < 0.01$). Countries with negative values for control of corruption were found to have cybercrime levels 40% higher on average. A comparative legal analysis of the cybersecurity systems of Japan, South Korea, and China demonstrated substantive differences in procedural mechanisms, sanctioning measures, and institutional architecture. The findings confirmed the significance of institutional quality for the effective protection of national cybersecurity and substantiate the need for a systematic modernisation of Kazakhstan's model through legislative codification, the establishment of a centralised coordination centre, the strengthening of sanctioning mechanisms, and the development of human capital

Keywords: personal data; law enforcement; critical infrastructure; sanctioning mechanisms; institutional quality; international coordination; data localisation

Introduction

The rapid development of digitalisation and information technologies in Central and East Asian states has generated a need to establish effective legal mechanisms for ensuring cybersecurity and protecting personal data. As of 2024, these countries are experiencing an escalation of cyber threats, reflected in the growing volume and sophistication of cyberattacks, rising losses from cybercrime, and increasing vulnerabilities within critical information infrastructure. According to the Asia Pacific Computer Emergency Response Team (APCERT, 2024), the number of registered cybersecurity incidents in the Asia-Pacific region rose by 23% compared with the previous year, while financial losses from cybercrime in several states more than doubled. Geopolitical transformations, particularly in the context of competition among major technological powers for influence in Central and East Asia, further heighten the relevance of

Suggest Citation:
Ismailova, G., & Kadirova, N. (2025). Cybersecurity law in Kazakhstan: A comparative analysis with East Asian practices. *Asian Journal of Criminal Justice and Forensic Studies*, 1(1), 35-51.

*Corresponding author

issues related to national cybersovereignty and cross-border data flows. The fragmented nature of existing legal regimes and the absence of unified approaches to cybersecurity regulation pose significant challenges for the economic integration and digital transformation of Central and East Asian states. The limited theoretical assessment of regional specificities in cybersecurity regulation highlights the need for a comprehensive examination of national legal frameworks and their alignment with international standards.

A comprehensive regional analysis of data-protection regimes in Central Asia was conducted by G. Greenleaf & T. Kaldani (2025), who found that all six countries in the region have enacted new or recently revised data-privacy laws, with the strongest legal systems observed in Uzbekistan, Mongolia, and Kazakhstan. The researchers noted that the enforcement of these laws remains at an early stage, characterised by low penalties for violations and limited evidence of compliance. The geopolitical context of regional cyberlaw development was examined by C. Zhang (2024), who demonstrated that China's privacy-protection strategy, combining a comprehensive regulatory system with government access to data, is reshaping global data-governance paradigms and generating new geopolitical fault lines. The author established that the Chinese approach, which prioritises state sovereignty over individual privacy, may serve as a potential model for governments seeking to maintain state control over data. This approach diverges significantly from Western models of data privacy and produces normative tensions with states that promote a more open digital economy.

A detailed examination of Kazakhstan's legislation on personal data protection was conducted by F. Syrlybayeva *et al.* (2024), who identified substantial deficiencies in the country's legal doctrine concerning the consolidation of fundamental principles governing the collection, processing, and storage of citizens' personal data. The authors established that the 2024 amendments to the Law of the Republic of Kazakhstan No. 94-V ZRK (2013), despite improving governance, do not comply with the requirements of the General Data Protection Regulation (GDPR) in several areas, including transparency and data-subject rights. A comparative legal analysis carried out by A. Amirov *et al.* (2024) confirmed the fragmented character of Kazakhstan's legislation and its partial alignment with European Union standards, with the researchers emphasising the importance of increasing public awareness of rights and obligations in the digital environment. Further theoretical development was provided by N.B. Kubanova (2025), who identified significant limitations within the existing personal data-protection system, which applies only to specific categories of information and fails to comprehensively address issues related to labour relations. The author argued for the development of specialised legislation and highlighted the importance of improving digital literacy to support the formation of a resilient digital ecosystem.

Systemic cybersecurity challenges in the region were examined comprehensively by M. Orumbayeva & A. Kurmangali (2022), who identified three principal obstacles to strengthening cyber defence: insufficient funding and limited access to technology, a shortage of qualified specialists, and a lack of transparency in digital information and public discourse regarding the role of digitalisation in society. The researchers established that even in Kazakhstan, one of the most technologically advanced states in the region, there are substantial shortcomings in antivirus equipment and software used by central and local government institutions. Empirical confirmation of these findings was provided by N. Kubanova *et al.* (2024), who identified a sharp increase in both the volume and complexity of cyberattacks in Kazakhstan, including 4,507 malware cases in 2024, a figure more than twice that of the previous year. The authors found that the small and medium-sized enterprise sector was the most vulnerable, while losses in the banking sector reached 1.5 billion tenge in the second half of 2024 alone. The study demonstrated that approximately 70% of successful intrusions were attributable to human factors, including insufficient staff qualifications and configuration errors.

Conceptual aspects of cybersecurity regulation were examined by Z.O. Kulzhabayeva (2024), who argued for a statutory differentiation between the concepts of "cybersecurity" and "information security" within the context of informatisation and proposed the introduction of definitions such as "cybersecurity threat" and "cybersecurity incident". She recommended expanding the powers of owners of critical information and communication infrastructure facilities to improve their capacity to respond effectively to cyber incidents. Technological dimensions of digital transformation, viewed through the implementation of blockchain technologies in Kazakhstan, were analysed by S. Zhamburbayeva & G.A. Ilsasova (2024), who identified potential applications of blockchain to enhance transparency, security, and data reliability across various sectors. The researchers identified the need to develop new legislative acts and to adapt existing regulatory documents in order to create an enabling legal environment for blockchain, emphasising the importance of international cooperation and the exchange of best practices in this domain. They also highlighted the advantages of blockchain technologies, including the reduction of human-error-related risks, lower operational costs, and enhanced security in data transmission.

An alternative perspective on the evolution of cyber strategy was presented by N. Katagiri (2022) through an examination of Japan's cybersecurity policy between 2017 and 2020. The author concluded that policy changes remained moderate due to the resilience of existing constraints on the use of force. The analysis demonstrated that Japan's traditionally defensive posture continued to underpin the deterrent nature of its cyber strategy, evident in the legal system's status-quo orientation and in the country's adherence to international expectations regarding responsible state behaviour in cyberspace. The study showed that structural influences on governmental cybersecurity activity are likely to emerge only in the long term, given Japan's preference for a fragmented approach to addressing persistent challenges in

cyberspace. This conservative stance stands in marked contrast to the more assertive cybersecurity strategies developing in Central Asian states and illustrates the diversity of national models for regulating cyberspace across the Asian region. At the same time, issues concerning the harmonisation of national cybersecurity legislation and the mechanisms of international cooperation among states in the region to counter cross-border cyber threats have remained insufficiently explored. This research aimed to identify avenues for modernising the national cybersecurity system of the Republic of Kazakhstan. The objectives were as follows:

1. To analyse the current state of Kazakhstan's national cybersecurity system, including its legal framework and the effectiveness of law enforcement;

2. To examine cybersecurity practices in Japan, South Korea, and China in order to identify successful elements suitable for adaptation;

3. To develop recommendations for modernising Kazakhstan's national cybersecurity system on the basis of the conducted analysis.

Materials and Methods

The study employed a comprehensive legal approach grounded in the conceptual frameworks of international law and comparative jurisprudence, supplemented by theoretical foundations in public administration and institutional analysis. Its theoretical basis was formed by doctrinal principles concerning the implementation of international cybersecurity standards in national legal systems and by concepts addressing the relationship between governance quality and the effectiveness of national cyber-defence systems. The research materials included Kazakhstan's regulatory acts on cybersecurity, official statistical data issued by state authorities, international rankings and indices, legislation of Asia-Pacific states, reports of national computer emergency response teams, as well as analytical publications produced by international organisations and leading law firms. The methodological framework was informed by theories of legal transformation in post-Soviet states, which enabled an assessment of the transition from fragmented to comprehensive cybersecurity systems under conditions of institutional reform.

The study was conducted in three sequential stages in accordance with its stated objectives. The first stage involved a legal analysis of Kazakhstan's cybersecurity regulatory landscape using the formal-legal method to examine the structure and content of the core legislative acts. The analysis covered the provisions of the Law of the Republic of Kazakhstan No. 418-V ZRK (2015), the Law of the Republic of Kazakhstan No. 94-V ZRK (2013) as amended in 2024, and the relevant chapters of the Criminal Code of the Republic of Kazakhstan No. 226-V KRZ (2014). Additional attention was given to the Code of the Republic of Kazakhstan No. 235-V KRK (2014) to assess administrative sanctions for violations in the field of cybersecurity, and to the Criminal Procedure Code of the Republic of Kazakhstan No. 231-V KRZ (2014) to understand procedural aspects of cybercrime investigations. Strategic documents, including Government Decree of the Republic of Kazakhstan No. 407 (2017) and Government Decree of the Republic of Kazakhstan No. 269 (2023), were examined. Analytical publications from leading law firms, including AEQUITAS Law Firm (2024) reports on doing business in Kazakhstan and S. Akhmetova (2024) materials on state supervision of personal data protection, were also utilised to assess enforcement practices and recent legislative developments. This comprehensive analysis aimed to identify gaps in legal regulation, evaluate the system of sanctioning mechanisms, and determine the extent to which national legislation corresponds to contemporary cybersecurity challenges.

The second stage involved an empirical analysis of the effectiveness of Kazakhstan's cybersecurity system using statistical and correlation-based methods. A quantitative assessment of the dynamics of cyber incidents was conducted on the basis of official data from the national response centre KZ-CERT, published by the Forum of Incident Response and Security Teams (n.d.). Statistical materials from the OSCE (Organization for Security and Co-operation in Europe) M. Stickings & J. Nosal (2024) concerning countercybercrime efforts in Central Asia were also examined. Official statistics from the State Technical Service (Cyber attacks of 2024…, 2025) on cyberattacks recorded in 2024, as well as judicial statistics reported by the Less than half of criminal cases… (2025), were processed. Additional data were drawn from the Committee for National Security of the Republic of Kazakhstan (2021) on the prevention of cyberattacks and from the F. Mukhametgali (2024) on court verdicts in cybercrime cases. A correlation analysis was employed to identify statistically significant associations between four key governance-quality indicators from the Worldwide Governance Indicators – Regulatory Quality, Rule of Law, Control of Corruption, and Political Stability and Absence of Violence/Terrorism (Worldwide Governance Indicators, 2024) – and cybercrime metrics, including the number of registered cybercrimes per 100,000 population and the percentage of cases resulting in convictions. Data from the NCSI (National Cyber Security Index, n.d.) were used to evaluate the overall condition of the national cybersecurity system. Official media reports on Kazakhstan's position in the 2024 Global Cybersecurity Index were examined (Abuova, 2024). The Global Cybercrime Report 2024… (2024) and ITU (International Telecommunication Union, 2020) data on international cybersecurity indicators for Asia-Pacific states were also analysed, enabling an assessment of Kazakhstan's standing relative to other countries in the region in terms of cyber-threat levels. Analytical materials on the economic losses caused by cybercrime, prepared by the Eurasian Research Institute (2025) and S. Kergroach *et al.* (2024), along with global statistics from Evolve Security on the cost of cybercrime, were reviewed. The regional report of the Asia Pacific Computer Emergency Response Team (APCERT, 2024) was additionally analysed to contextualise Kazakhstan's indicators within the broader Asia-Pacific cybersecurity landscape.

Data from the Ministry of Education and Science of the Republic of Kazakhstan on the number of cybersecurity education programmes available on the Univision.kz platform (n.d.a; n.d.b) as of 2024 were used to assess the state of human-capital development in this field.

The third stage involved a comparative legal analysis of national cybersecurity systems to identify key elements of successful regulatory models. Japan's legal system was examined through an analysis of the Act of Japan No. 104 (2014) as amended in 2019, the Act of Japan No. 57 (2003) together with the official Guidelines of the Personal Information Protection Commission (2022), and the Act of Japan No. 128 (1999) to understand the criminal-law mechanisms involved. Official documents of the Government of Japan (n.d.) concerning policies for the protection of critical infrastructure were examined. South Korean legislation was analysed, including the Act of the Republic of Korea No. 14080 (2016), Act of the Republic of Korea No. 14122 (2016) and Act of the Republic of Korea No. 19234 (2023), which together form the basis of the Data 3 Act package of 2020, with the most recent amendments in 2024. The national cybersecurity strategy of South Korea was reviewed using materials from the South Korea's 2024 Cyber Strategy: A Primer (2024). Chinese legislation was studied through a review of key laws, including the Cybersecurity Law of the People's Republic of China (Creemers *et al.*, 2018), Data Security Law of the People's Republic of China No. 84 (2021), and Personal Information Protection Law of the People's Republic of China No. 91 (2021), as well as regulatory documents issued by the CAC (Cyberspace Administration of China) (Regulations on the Management of Online Data…, 2021) and relevant provisions of the Criminal Law of the People's Republic of China (1979) concerning criminal liability for cyber offences. Analytical materials from international law firms, including Baker McKenzie (2025), were utilised to understand practical aspects of legislative implementation. Documents from the Council of Europe (2022; 2023; 2024) were examined to assess Kazakhstan's status with regard to the Budapest Convention on Cybercrime and mechanisms of international legal assistance, including materials on the network of 24-hour contact points and the Second Additional Protocol on electronic evidence. The bilateral agreement on mutual legal assistance between Kazakhstan and the United States of America was examined (International treaty UK/Kazakhstan TS No. 25/2016, 2016). A comparative analysis of operational models of incident response centres was conducted through a study of the Japan Computer Emergency Response Team Coordination Center (JPCERT, 2024) based on the organisation's official information and international cybersecurity indicators for Japan (National Cyber Security Index, n.d.; International Telecommunication Union, 2020), as well as statistical reports from the Coordination Center. The South Korean centre KrCERT/CC was analysed using the NATO Cooperative Cyber Defence Centre of Excellence (Cho, 2022) report, alongside the activities of Kazakhstan's KZ-CERT, drawing on materials from, which allowed for an evaluation of operational capabilities, resource provision, and the effectiveness of national incident response systems from a comparative perspective.

Results

Legal framework and law enforcement in Kazakhstan

An analysis of current legislation in the Republic of Kazakhstan revealed a fragmented legal system, characterised by the absence of a single codified act and a multiplicity of regulatory documents with varying legal force. The legal foundation of Kazakhstan's cybersecurity framework is formed by two primary legislative acts: the Law of the Republic of Kazakhstan No. 418-V ZRK (2015) of 24 November 2015, and the Law of the Republic of Kazakhstan No. 94-V ZRK (2013) of 21 May 2013, as amended in 2024. The Law of the Republic of Kazakhstan No. 418-V ZRK (2015) establishes the legal foundations for the creation, operation, and protection of information systems. It defines the concept of critical information infrastructure (CII), obliges CII operators to register, develop and implement security policies, and to report incidents to the authorised body. Article 1 of the Law defines information security as the state of protection of information and information systems against unauthorised access, use, disclosure, destruction, modification, or loss. Article 29 stipulates that owners of information systems are required to ensure the protection of information in accordance with the legal requirements on information security and personal data. At the same time, legal analysis reveals that the Law contains numerous references to subordinate regulations and grants wide discretion to executive authorities regarding specific technical standards. Notably, the text does not include provisions on cyber incidents, procedures for their investigation, or mechanisms for interagency coordination in responding to cyberattacks (AEQUITAS Law Firm, 2024).

The Law of the Republic of Kazakhstan No. 94-V ZRK (2013) establishes a regime for the localisation of personal data within Kazakhstan and introduces mechanisms for reporting security breaches. Article 15 provides that the personal data of citizens of the Republic of Kazakhstan must be stored in personal data databases located on Kazakhstani territory, while Article 17 permits the transfer of personal data abroad only if the receiving state provides an adequate level of data protection or if the data subject has provided written consent. The 2024 amendments introduced the concept of a "personal data security breach", obliging organisations to report leaks to the Ministry of Digital Development and Innovations, prohibiting the collection of physical document copies, and establishing a 33-point checklist to verify compliance with requirements (Akhmetova, 2024). Article 191 of the Law, in its revised version, requires personal data operators to notify the authorised body of a security breach within one working day of its detection. The notification must include information on the nature of the breach, the number of data subjects affected, potential consequences, and measures taken to address the

incident (AEQUITAS Law Firm, 2024). However, enforcement practice reveals a lack of effective mechanisms to ensure compliance with localisation requirements, including audit procedures for data centres, the maintenance of storage registries, and the application of sanctions for violations.

Strategic planning in the field of cybersecurity is carried out through the national programmes set out in Government Decree of the Republic of Kazakhstan No. 407 (2017) for 2017-2021 and Government Decree of the Republic of Kazakhstan No. 269 (2023) for 2023-2029. The 2017 Cyber Shield of Kazakhstan concept defines cybersecurity as a key condition for joining the club of the most developed nations and sets out objectives to raise public awareness, develop domestic information and communication technology (ICT) products, improve law enforcement operations, and establish an adaptive information-security management system for critical information infrastructure. The 2023-2029 strategy envisages the implementation of a risk-based approach to cybersecurity management, the development of public-private partnerships, and the harmonisation of national legislation with international standards, including the establishment of a unified national centre for cyber-threat monitoring. The digital transformation concept allocates responsibilities among ministries and records achievements such as near-complete internet coverage, growth in e-commerce, and the launch of digital farms. However, as a government decree, it can be easily amended and does not carry the force of law (Government Decree of the Republic of Kazakhstan No. 269, 2023). Legal analysis of these documents indicates a largely declarative character, as they lack measurable performance indicators and specific mechanisms for achieving the stated objectives. Kazakhstan's criminal legislation contains a dedicated Chapter 9, "Criminal Offences in the Field of Information Technologies", which includes Articles 205-207 of the Criminal Code of the Republic of Kazakhstan No. 226-V KRZ (2014). The structure of criminal and administrative liability for cybercrime in Kazakhstan is summarised in Table 1.

Table 1. Sanctioning provisions of Kazakhstan's criminal and administrative legislation in the field of cybersecurity

0,25 пт	Qualification	Sanction	Typical verdicts/examples
Art. 205-1, Criminal Code of the Republic of Kazakhstan (2014)	Unauthorised access to computer information (basic form)	Fine of 200-500 monthly calculation indices (MCI), or corrective labour up to 1 year, or restriction of liberty up to 2 years	In 2024, 24 incidents were prosecuted under Art. 205, nearly half carried over from previous years
Art. 205-2, Criminal Code of the Republic of Kazakhstan	Unauthorised access for material gain or by a group of persons	Fine of 500-1000 MCI, or restriction of liberty for 2-4 years, or detention up to 6 months	In January 2025, the Taldykorgan court fined two individuals 300 MCI each for unauthorised access to the Ministry of Health information systems
Art. 205-3, Criminal Code of the Republic of Kazakhstan	Unauthorised access causing significant damage or committed against CII	Fine of 1000-2000 MCI, or restriction of liberty for 3-5 years, or imprisonment up to 5 years	Specific verdicts under this provision are not publicly available
Art. 205-4, Criminal Code of the Republic of Kazakhstan	Unlawful destruction or modification of information relating to CII with serious consequences	Imprisonment for 4-6 years	In 2024, 24 cases were registered under all parts of the Art. 205, but only a portion were brought to court
Art. 207-1, Criminal Code of the Republic of Kazakhstan	Violation of rules for operating computer systems or their networks (basic form)	Fine of 100-200 MCI, or corrective labour up to 1 year, or restriction of liberty up to 2 years	In 2024, only five incidents were prosecuted under Art. 207
Art. 207-2, Criminal Code of the Republic of Kazakhstan (2014)	Violation of system operation causing significant damage or affecting CII	Fine of 200-500 MCI, or restriction of liberty for 2-5 years, or imprisonment up to 4 years	In December 2020, the Saryarkinsky District Court sentenced an individual for a coordinated distributed denialofservice attack on the electronic public procurement system to 2 years' restriction of liberty and barred him from participating in electronic public procurement activities for 3 years
Art. 210, Criminal Code of the Republic of Kazakhstan No. 226-V KRZ (2014)	Creation, use, or distribution of malicious computer programs or software products	Fine of 200-500 MCI, or corrective labour up to 1 year, or restriction of liberty up to 3 years	In August 2024, the Kostanay Regional Court sentenced a 24year-old resident for distributing malware to 1 year's restriction of liberty, 100 hours of compulsory labour, a fine of 15 MCI, and confiscation of computer equipment
Arts. 79, 641, Code of the Republic of Kazakhstan No. 235-V KRK (2014)	Violation of legislation on personal data and its protection, including rules on the storage and processing of personal data	Fine for individuals: 10-20 MCI; for officials: 30-50 MCI; for organisations: up to 2000 MCI	Statistics on the application of administrative sanctions are limited in publicly available sources

Note: as of 2024, 1 MCI equals 3,692 KZT (approximately 7.70 USD at the November 2024 exchange rate)
Source: compiled by the authors based on Al-Farabi Kazakh National University (n.d.), Criminal Code of the Republic of Kazakhstan No. 226-V KRZ (2014), Criminal Procedure Code of the Republic of Kazakhstan No. 231-V KRZ (2014), Committee for National Security of the Republic of Kazakhstan (2021), F. Mukhametgali (2024), Less than half of criminal cases… (2025), Committee of National Security of the Republic of Kazakhstan (2025)

Analysis of Table 1 indicates that sanctions for cybercrime in Kazakhstan are relatively mild compared with the potential losses caused by such offences. Basic offences carry fines ranging from 200 to 500 MCI (approximately 1,540 USD to 3,850 USD) or restriction of liberty for up to two years, while harsher penalties are applied only in the presence of aggravating circumstances. Judicial practice demonstrates a predominance of suspended sentences and restrictions of liberty over actual imprisonment, which diminishes the deterrent effect of criminal sanctions. For example, even in a high-profile case involving a distributed denial-of-service (DDoS) attack on the electronic public procurement system, which caused economic losses by delaying 7,901 government procurements worth 164 billion KZT, the offender received only two years' restriction of liberty without actual incarceration (Committee for National Security of the Republic of Kazakhstan, 2021).

The institutional structure for cybersecurity is characterised by a multi-level organisation with functions distributed across various state bodies, lacking a clearly defined central coordinator. The Committee for Information Security under the Ministry of Digital Development, Innovations, and Aerospace Industry (MDDIAI) sets policy, develops standards, monitors compliance, and coordinates the activities of the national centre KZ-CERT (National Cyber Security Index, n.d.). The national company State Technical Service acts as the operator of the national cyber-attack response centre, monitoring Kazakhstan's segment of the Internet, analysing malicious software, and coordinating responses to cyber incidents. Within this structure, KZ-CERT collects and analyses information on cyber incidents, provides recommendations for addressing vulnerabilities, and conducts educational outreach among users of information systems. The Committee for National Security is responsible for cryptographic protection and countering cyber-espionage, as well as the security of facilities containing state secrets. It conducts operational and investigative activities and pre-trial investigations of cybercrime in accordance with the Criminal Procedure Code of the Republic of Kazakhstan No. 231-V KRZ (2014). In the field of personal data, the authorised body is the Committee for Information Security of the MDDIAI, which, under the Law of the Republic of Kazakhstan No. 94-V ZRK (2013) and the Code of the Republic of Kazakhstan No. 235-V KRK (2014), supervises compliance, considers complaints from data subjects, and initiates administrative proceedings against violators. However, Kazakhstan lacks a single, centralised coordination centre comparable to Japan's National Information Security Centre (NISC) and does not have an overarching cybersecurity strategy. As a result, the functions of different agencies often overlap, leading to inefficient use of resources and slower responses to cyber incidents.

Kazakhstan is not yet a Party to the 2001 Budapest Convention on Cybercrime: on 19 April 2023, the country was invited to accede (Council of Europe, 2023), with the invitation valid until April 2028. As of November 2025, the ratification instrument has not been deposited, so Kazakhstan is not yet part of the Convention's network of 24/7 points of contact (POC) and cannot sign the Second Additional Protocol on Electronic Evidence (Council of Europe, 2022). Nevertheless, the MDDIAI and the Ministry of Internal Affairs are cooperating with the Council of Europe under the Octopus project to align national legislation with the Convention and to establish a national 24/7 POC (Council of Europe, 2024). For international legal assistance (MLAT), Kazakhstan relies on regional agreements within the Commonwealth of Independent States (CIS) and bilateral treaties on mutual legal assistance, including with the United States of America (signed 20 February 2015, entered into force 6 December 2016) (International treaty UK/Kazakhstan TS No.25/2016, 2016), while urgent requests are processed through the National Central Bureau of INTERPOL and KZ-CERT channels.

Trends in cyber incidents and investigations (2019-2024)

KZ-CERT statistics demonstrate a sustained increase in the number of cyber incidents in Kazakhstan between 2019 and 2024, with an average annual growth rate of 14.5%, significantly outpacing the pace of the country's digitalisation of the economy. According to the OSCE (Stickings & Nosal, 2024), the number of registered cybercrimes in Kazakhstan rose from 589 cases in 2018 to 21,479 in 2021, representing an increase of more than 36-fold. In 2019, 20,800 incidents were recorded, of which 17,300 involved botnet activity, 201 were DDoS attacks, and the remainder comprised other types of cyber threats, including phishing, malware, and attempts at unauthorised access. Official data from the Cyber attacks of 2024… (2025) for 2024 records over 41,000 incidents, approximately 66% of which involved malware infections, around 20% were phishing campaigns, 8% were DDoS attacks, and 6% consisted of other threat types. According to the Cyber and Digital Security forum organised by the State Technical Service in 2024, 740 million cyberattacks were blocked, and more than 6,500 DDoS attacks on critical information infrastructure were successfully repelled. Sectoral analysis shows that the most targeted sectors are financial services (28% of incidents), public administration (22%), telecommunications (18%), and energy (15%) (Nguyen *et al.*, 2021).

Financial losses from cybercrime illustrate the scale of the problem for Kazakhstan's economy. The 2025 report of the Eurasian Research Institute provides specific figures: in 2023, citizens lost over 17.5 billion KZT (approximately 37 million USD) due to digital fraud, and in 2024, 11,765 cases of online fraud were registered, only 152 more than in 2023, representing an increase of 1.31% (Eurasian Research Institute, 2025). Frauds included phishing, counterfeit banking websites, investment scams, and credential theft. Compared with a population of approximately 20 million, these figures may appear modest; however, experts consider the actual number of incidents to be substantially higher due to the low rate of reporting to the police. Global losses from cybercrime exceeded 8 trillion USD in 2022 and are projected to reach 10.5 trillion USD by 2025, reflecting an

annual growth rate of 15% (Hernandez, n.d.). At the enterprise level, according to the OECD, the median cost of a ransomware attack can reach up to 1.2 million USD, while a data breach may incur losses of up to 1.6 million USD (Kergroach *et al*., 2024).

Judicial statistics confirm systemic problems in law enforcement and cybercrime investigation, with a low proportion of cases reaching court. According to the Less than half of criminal cases… (2025), in 2024, 99 criminal offences in the information and communication technology sector were registered in Kazakhstan; however, only 44 were investigated, and merely 36 cases were referred to court, representing 36% of the registered incidents. The largest share of registered offences comprised 70 cases of information destruction or modification, whereas only five incidents were prosecuted under Article 207 of the Criminal Code of the Republic of Kazakhstan No. 226-V KRZ (2014) for disrupting the operation of an information system or telecommunications network, and 24 cases under Article 205 for unauthorised access to an information system, with nearly half of these cases carried over from previous years. Twenty-eight cases were closed due to statute of limitations or the inability to identify the perpetrator, highlighting difficulties in tracing offenders and collecting digital evidence.

A detailed analysis of individual court cases illustrates characteristic issues within Kazakhstan's criminal justice system regarding cybercrime. In December 2020, the Saryarkinsky District Court of Nur-Sultan convicted an individual for a coordinated DDoS attack on the electronic government procurement system in May of the same year (Committee for National Security of the Republic of Kazakhstan, 2021). The cyberattack caused the goszakup.gov.kz platform to become non-operational, resulting in the postponement of 7,901 government procurement procedures valued at 164 billion tenge due to the technical impossibility of conducting electronic tenders as scheduled. The perpetrator, who sought to gain advantages in government procurement, was identified by the Committee for National Security with the assistance of the Electronic Finance Centre. Following a computer-technical examination, the defendant was found guilty under Part 2, Paragraph 1 of Article 207 of the Criminal Code and sentenced to two years of restricted liberty, with a three-year prohibition on engaging in activities related to electronic government procurement (Committee for National Security of the Republic of Kazakhstan, 2021). Notably, even in the face of significant economic damage, the court imposed a relatively lenient sentence without actual imprisonment.

Another case occurred in the Kostanay Region in August 2024, where a local court convicted a 24-year-old resident for distributing malicious software online. The perpetrator, whose activities involved spreading viruses to harvest users' personal data and offering paid tutorials on creating malware, was stopped by the Department of the Committee for National Security and the Police Department. The court found him guilty under Part 1 of Article 210 of the Criminal Code and imposed a sentence of one year of restricted liberty, 100 hours of compulsory labour, a fine of fifteen MCI, and the confiscation of computer equipment (Mukhametgali, 2024). This case illustrates a typical pattern: even when guilt is established and the offender identified, courts often impose suspended or lenient sentences, which do not generate a sufficient deterrent effect.

Formally, criminal liability for unauthorised access, the distribution of malicious software, and fraud is established in the Criminal Code; however, the number of convictions for cybercrimes recorded in the judicial registry remains limited. This indicates challenges in the organisation of investigations, the insufficiency of specialised units, and difficulties in collecting digital evidence. Enforcement effectiveness is further undermined by the lack of specialised training for investigators, the limited technical capacity of expert institutions, and the complexity of international cooperation in investigating cross-border cybercrime.

Correlation between governance quality and cybercrime levels

Governance indicators in Kazakhstan reveal systemic deficiencies in institutional capacity within the cybersecurity sector, negatively affecting the effectiveness of measures to combat cybercrime (Table 2). The correlation between the number of cybercrimes and governance indicators shows a statistically significant negative relationship ($r = -0.67$, $p < 0.01$). This suggests that countries with low rule of law and regulatory quality scores experience higher success rates of cyberattacks and lower effectiveness of law enforcement in investigating cybercrime. Countries with a "Control of Corruption" indicator below zero exhibit, on average, a 40% higher level of cybercrime compared with countries displaying positive values for this indicator.

Table 2. Comparative assessment of Worldwide Governance Indicators, 2023

Country/ Indicator	Regulatory Quality	Rule of Law	Control of Corruption	Political Stability & Absence of Violence/Terrorism
Kazakhstan	+0.07% / 53.3% (+3.3 pp)	-0.45% / 36.8% (-13.2 pp)	-0.27% / 47.2% (-2.8 pp)	-0.27% / 36.5% (-13.5 pp)
Japan	+1.47% / 92.5% (+42.5 pp)	+1.54% / 92.5% (+42.5 pp)	+1.40% / 90.1% (+40.1 pp)	+0.95% / 81.5% (+31.5 pp)
South Korea	+1.12% / 84.9% (+34.9 pp)	+1.25% / 85.8% (+35.8 pp)	+0.89% / 79.7% (+29.7 pp)	+0.61% / 68.2% (+18.2 pp)
China	-0.36% / 38.7% (-11.3 pp)	-0.04% / 52.8% (+2.8 pp)	-0.01% / 54.2% (+4.2 pp)	-0.51% / 25.1% (-24.9 pp)

Note: values are presented as Estimate (range -2.5 to +2.5) / Percentile Rank (0-100%), with deviations from the median percentile (50%) shown in parentheses. Percentile ranks indicate the proportion of countries with lower scores; higher values correspond to better governance quality. Deviations exceeding ±25 percentile points (pp) from the global median are analytically significant for the formulation of policy recommendations

Source: compiled by the authors based on Worldwide Governance Indicators (2024)

A comparative analysis of the Worldwide Governance Indicators presented in Table 2 reveals notable differences in the quality of the institutional environment among the countries studied, which directly correlates with the effectiveness of their cybersecurity systems. Japan and South Korea exhibit high governance quality across all dimensions, creating a favourable institutional environment for effective law enforcement and coordination between the public and private sectors in the field of cybersecurity. Kazakhstan, by contrast, displays predominantly negative values for most indicators, particularly in terms of rule of law, control of corruption, and political stability. This reflects structural institutional weaknesses that hinder the effective implementation of cybersecurity policy and reduce business confidence in state initiatives. The low rule of law indicates difficulties in ensuring legislative compliance and the efficiency of the judicial system. China occupies an intermediate position, with relatively stronger institutional quality indicators than Kazakhstan. This partly explains the Chinese system's ability to maintain centralised control over cyberspace, despite limitations in political stability.

International cybersecurity rankings place Kazakhstan at an average level, indicating scope for significant improvement. According to the 2024 Global Cybersecurity Index compiled by the International Telecommunication Union (ITU), Kazakhstan scored 94.04 out of a possible 100 points, placing it in the second group of "emerging countries". The country achieved full marks of 20 for legal and cooperative measures, 19.38 for technical measures, 18.3 for organisational measures, and 16.36 for capacity development (Abuova, 2024). This outcome indicates that the state has invested in building a regulatory and coordination framework, but requires strengthening of human resources, as the lowest score was recorded in capacity development. According to the NCSI, Kazakhstan ranks 38th with a score of 73.33, below the East Asian countries: South Korea ranks 22nd with 83.33 points, while China is 53rd with 60.00 points (National Cyber Security Index, n.d.). For Japan, the International Telecommunication Union (2020) places the country 7th in the Global Cybersecurity Index with a score of 97.82. NCSI reports a score of 63.64 for Japan, corresponding to 52nd in the global ranking. The MixMode analytical report, based on a comprehensive analysis of four indices, indicates Japan's cyber resilience index at 82.29 and an overall cybersecurity score of 88.77, reflecting the country's strong technical and organisational base (Global Cybercrime Report 2024…, 2024).

Sociological research on public awareness in Kazakhstan indicates relatively high levels of citizen knowledge about cyber threats, albeit with a notable gap between knowledge and behaviour. A 2023 government survey found that 80.4% of respondents were aware of the existence of cyber threats, 74.64% could identify phishing messages, and 90.52% possessed skills to protect personal data on social networks (Eurasian Research Institute, 2025). In 2024, the Ministry of Digital Development launched an interactive platform, Cyberlabyrinth, where schoolchildren and university students learn the basics of cyber hygiene through gamified activities and receive certificates. The programme has become popular and contributed to growing interest in information technology careers. Cybersecurity weeks are also actively conducted, involving banks, telecom operators, and civil society organisations. However, high awareness does not necessarily translate into behavioural change, as many citizens continue to use weak passwords, install pirated software, and connect to unsecured Wi-Fi networks. According to the Ministry of Education and Science (Univision.kz, n.d.a, n.d.b), by 2024, Kazakhstan offered only 12 undergraduate and eight postgraduate programmes in information security, which does not meet labour market demand. At the same time, there were approximately 1,500 certified cybersecurity specialists, an insufficient number to meet the needs of both the public and private sectors.

Comparative legal analysis of the cybersecurity systems of Kazakhstan, Japan, South Korea, and China

The Japanese cybersecurity model is founded on comprehensive legislation with centralised coordination and principles of shared responsibility. Act of Japan No. 104 (2014), as amended in 2019, establishes the fundamental principles and identifies responsible entities, emphasising the protection of citizens' lives and rights, economic prosperity, and national security, while promoting the free and secure flow of information. Between 2020 and 2022, the Act on the Protection of Personal Information (APPI) was significantly updated. Amendments effective from 1 April 2022 expanded obligations regarding data breach notifications, tightened requirements for cross-border transfers of personal information, and substantially increased the maximum fines for legal entities (up to 100 million JPY) for non-compliance with directives issued by the Personal Information Protection Commission (PPC). Article 1 of the Act establishes the aim of ensuring a safe and peaceful society through comprehensive and effective cybersecurity measures, while Article 2 defines cybersecurity as the prevention of leaks, loss, destruction, and other incidents concerning electronic information and information systems, as well as the maintenance of stable system operations and their effective utilisation. The law allocates responsibilities among the national government, local authorities, operators of critical information infrastructure, enterprises, and citizens, delineating the role of each. It also mandates the development of a national cybersecurity strategy and establishes a Cybersecurity Headquarters under the Cabinet of Ministers. In practice, these functions are carried out by the National Centre of Incident Response and Strategic Coordination (NISC), which coordinates policy, develops standards for government systems, conducts audits, and manages the government network monitoring centre (Government of Japan, n.d.). In 2024, the Japanese government updated the Critical Infrastructure Protection Policy, adding ports and harbours to the list of critical sectors, thereby expanding the scope of responsibility for logistics service providers. According to JPCERT/CC (Japan Computer

Emergency Response Team Coordination Center), in 2023 alone, the organisation received 65,669 reports of computerrelated incidents from Japan and abroad, reflecting both the scale of cyberattacks and the key role of the national Computer Security Incident Response Team (CSIRT) in the practical implementation of state cybersecurity policy (JPCERT Coordination Center, 2024).

The South Korean system is characterised by comprehensive regulatory governance through a combination of specialised laws, mandatory standards, and active international cooperation. The legal framework is centred on three principal data laws: the Personal Information Protection Act (PIPA), including Act of the Republic of Korea No. 19234 (2023); the Information and Communications Network Act (Network Act), with one of the key versions being Act of the Republic of Korea No. 14080 (2016); and the Credit Information Use and Protection Act (Act of the Republic of Korea No. 14122, 2016). The 2020 amendments to these three acts, known collectively as the Data 3 Act package, centralised regulatory authority over privacy by transferring the previously fragmented functions of the Ministry of the Interior and the Korea Communications Commission to the unified Personal Information Protection Commission (PIPC), elevating its status as the central supervisory body for personal information protection. The PIPA serves as the foundational privacy law, establishing principles of data minimisation, legality, and transparency, as well as requirements for obtaining consent from data subjects. The Network Act, in turn, regulates the activities of telecommunications service providers, obliging them to implement measures to prevent data leaks, combat spam, follow incident reporting procedures, and granting authorities the power to issue orders to rectify violations (Baker McKenzie, 2025). Following the amendments to the Network Act, network operators and online service providers are required to notify affected users immediately in the event of a personal data breach and submit an initial report to the Korea Communications Commission or the Korea Internet & Security Agency within 24 hours of detecting the incident. Under the general PIPA framework, a report must be submitted to the PIPC and data subjects informed no later than 72 hours after the breach is discovered. Article 44-7 of the Information and Communications Network Act (ICNA) prohibits the dissemination of unlawful information that harms minors or infringes the rights of third parties, granting the Korea Communications Commission the authority to issue orders for its removal. Article 45 establishes obligations for information and communications service providers to implement technical and administrative measures to protect users' personal information (Anderson *et al*., 2015). In 2024, amendments to the Network Act strengthened measures against illegal spam, simplified the certification process for the Information Security Management System (ISMS), and granted authorities the power to issue orders to rectify violations and impose fines on non-compliant operators. The same year, the National Cybersecurity Strategy 2024 was adopted, explicitly identifying North Korea as a primary threat and emphasising the zero-trust principle. The strategy introduces a classification of incidents by severity and obliges organisations to report breaches within prescribed timeframes (South Korea's 2024 Cyber Strategy: A Primer, 2024).

The Chinese cybersecurity model is characterised by a centralised regulatory approach to cyberspace, underpinned by a comprehensive legislative framework that includes the Cybersecurity Law of the People's Republic of China (Creemers *et al*., 2018), the Law of the People's Republic of China No. 84 (2021), and the Personal Information Protection Law of the People's Republic of China No. 91 (2021). The central coordinator of China's cybersecurity framework is the CAC, which holds extensive authority over oversight, certification, and enforcement of sanctions. The Chinese model imposes stringent data localisation requirements: operators of critical information infrastructure must store personal data and "important information" collected within the territory of the People's Republic of China on servers located domestically. Cross-border data transfers are permitted only after undergoing a state security assessment, creating additional barriers and costs for international companies providing digital services to Chinese users. These restrictions are directly linked to the doctrine of "cyber sovereignty" enshrined in the Cybersecurity Law, under which the state asserts full sovereignty over its national cyberspace and uses data flow regulation as a tool to protect national security and establish domestic rules for the global digital order. The Multi-Level Protection Scheme (MLPS 2.0) establishes a graduated classification of information systems across five levels of criticality, with corresponding requirements for certification, technical protection, and regular inspections (Regulations on the Management of Online Data…, 2021). A comparative analysis of procedural and sanctioning mechanisms in the cybersecurity legal frameworks of the countries studied is summarised in Table 3. The comparative analysis of procedural mechanisms in Table 3 reveals fundamental differences in approaches to ensuring cybersecurity and their alignment with the maturity of legal systems. The South Korean and Chinese systems are the most structured, featuring clear procedural frameworks with specific deadlines and enforcement mechanisms. The Chinese model additionally relies on data localisation requirements and the principle of cyber sovereignty, which significantly affect the ability of international companies to transfer user data abroad. The Japanese model is characterised by greater flexibility and an emphasis on voluntary cooperation, reflecting a high level of trust between the state and the private sector. Kazakhstan's system exhibits the greatest fragmentation in procedural mechanisms, with reporting deadlines limited solely to the sphere of personal data and lacking comprehensive requirements for CII. A pronounced disparity exists between the potential scale of damage from cyber incidents and the sanctioning mechanisms in Kazakhstan: the maximum administrative

fine is only 15,200 USD, whereas in South Korea and China, fines may reach millions of dollars or a percentage of a company's global turnover. This underscores the need for a fundamental overhaul of approaches to deterring cybercrime and ensuring operator accountability for compliance with cybersecurity requirements.

Table 3. Comparative analysis of procedural and sanctioning mechanisms in cybersecurity legal frameworks

Country	Mandatory incident notification period	Maximum administrative fine for organisations	Maximum criminal penalty for unauthorised access	Personal data localisation requirement	Central coordinator/ regulator	Sources
Kazakhstan	1 working day to the Ministry of Digital Development, Innovation and Aerospace Industry	Up to 2,000 monthly calculation indices – approximately 7.3 million KZT (≈ 15,200 USD) for serious personal data violations	Imprisonment up to 7 years	Yes; storage restricted to the territory of the Republic of Kazakhstan	Information Security Committee of the Ministry of Digital Development, Innovation and Aerospace Industry + KZCERT	Arts. 19-1, 15 Law of the Republic of Kazakhstan No. 94-V ZRK (2013); Arts. 79, 641 Code of the Republic of Kazakhstan No. 235-V KRK (2014); Art. 205(4) Criminal Code of the Republic of Kazakhstan No. 226-V KRZ (2014)
Japan	Preliminary notification: 3-5 days; final notification: up to 30 days	100 million JPY (≈ 660,000 USD) for corporations	Up to 3 years' imprisonment or a fine of up to 1 million JPY (≈ 6,600 USD)	No; crossborder transfers allowed with consent and recipient obligations	Cybersecurity Strategic Headquarters of the Cabinet + Personal Information Protection Commission	Guidelines of the Personal Information Protection Commission for the Act on the Protection of Personal Information (2022); Art. 832 Act of Japan No. 57 (2003); Art. 11 Act of Japan No. 128 (1999); Act of Japan No. 104 (2014); Government of Japan (n.d.)
South Korea	Immediate to users; within 24 hours to the Korea Communications Commission / Korea Internet & Security Agency (Network Act); within 72 hours to the PIPA	Up to 3% of global turnover or 3 billion KRW (≈ 2 million USD) for serious violations	Up to 5 years' imprisonment or a fine of 50 million KRW (≈ 35,700 USD)	No general requirement; consent of the data subject and specific contractual guarantees are required	Korea Internet & Security Agency / PIPC	Arts. 64-2, 71 Act of the Republic of Korea No. 14080 (2016, amended 2024); Act of the Republic of Korea No. 19234 (2023)
China (PRC)	Initial notification within 8 hours; full report within 5 working days	Up to 50 million CNY or 5% of annual turnover (≈ 7 million USD)	5-7 years' imprisonment for serious cyberattacks	Yes; for critical information infrastructure – storage within China and prior state security assessment for export	CAC	Regulations on the Management of Online Data... (2021); Art. 40, 66 Personal Information Protection Law of the People's Republic of China No. 91 (2021); Art. 286 Criminal Law of the People's Republic of China (1979); Art. 37 Cybersecurity Law of the People's Republic of China (Creemers *et al.*, 2018)

Note: maximum sanctions listed relate to the basic offence of "unauthorised access" and may increase under aggravating circumstances. The Act on the Protection of Personal Information refers to the Japanese law on the protection of personal information

Source: compiled by the authors

Functional analysis of incident response centres highlights significant differences in operational capacity, resource allocation, and overall effectiveness compared with Kazakhstan's KZ-CERT. Japan's JPCERT/CC, established in 1996, was the country's first Computer Security Incident Response Team (CSIRT) and effectively functions as a national "CSIRT centre". It coordinates interaction among network service providers, software developers, government agencies, and industry associations and played a key role in forming the Asia Pacific Computer Emergency Response Team (APCERT) network. The organisation receives information on incidents and malware from global partners, conducts technical and threat analyses, rapidly disseminates relevant data to stakeholders, and coordinates responses with national and international CSIRTs. JPCERT/CC operates as a neutral and independent entity, free from governmental control (Japan Computer Emergency Response Team Coordination Center, n.d.). Its statistics demonstrate the effectiveness of Japan's system: in 2023, the centre received 65,690 incident reports and handled 19,720 coordination cases, reflecting a highquality filtering and response process with a 30% handling rate (JPCERT Coordination Center, 2024).

South Korea's KrCERT/CC (Korea Computer Emergency Response Team Coordination Center), operating under the Korea Internet & Security Agency (KISA), offers a wide range of services. It provides consultation and receives reports on vulnerabilities and incidents, issues timely recommendations for vulnerability remediation to the private sector, assists with inspections of personal computers and Internet of Things (IoT) devices, supports small and medium-sized enterprises, strengthens website security, organises cyber training, and shares threat intelligence with private companies and academic institutions (Cho, 2022). KrCERT also monitors malware infections on over four million Korean websites and employs an automated Cyber Threat Analysis System (C-TAS) for data sharing. By comparison, Kazakhstan's KZ-CERT holds national and governmental authority and is responsible for every host or subnet connected to the Kazakh segment of the Internet (Forum of Incident Response and Security Teams, n.d.). However, it suffers from limited human and financial resources, lacks its own earlywarning system, and publishes insufficient information on incidents.

Recommendations for modernising Kazakhstan'snational cybersecurity system

The results of the comparative analysis allow the identification of key elements of successful cybersecurity systems in East Asian countries and inform concrete recommendations for Kazakhstan. All three countries demonstrate the presence of comprehensive framework laws or interconnected legislative acts covering both cybersecurity and personal data protection. Japan and China have enacted separate statutes that define core principles and establish coordinating authorities, whereas South Korea relies on several specialised laws complemented by a national strategy. The central role of a specialised coordinating body is evident in the functioning of Japan's NISC for strategic planning and coordination, the Cybersecurity Council under the President in South Korea, and CAC, all of which have the authority to issue binding directives, conduct audits, and allocate resources. Mandatory certification and standardisation systems are characterised by differing approaches: South Korea has implemented compulsory ISMS certification for network operators, China has introduced the MLPS, and Japan sets standards for government systems. Based on these observed patterns and the identified differences between national cybersecurity regulatory models, the following priority directions are proposed for modernising Kazakhstan's system.

The foremost task in modernising the national cybersecurity system is the codification of legislation to eliminate fragmented regulation and establish a unified legal framework. By the end of 2026, it is advisable to draft and submit to Parliament a single foundational law, On Cybersecurity, which integrates provisions of the current Law of the Republic of Kazakhstan No. 418-V ZRK (2015) and Law of the Republic of Kazakhstan No. 94-V ZRK (2013), supplemented with specific provisions on cyber-incident response procedures, interagency coordination mechanisms, and requirements for operators of CII. The proposed legislation should set clear deadlines for reporting different types of incidents, specifically no more than 24 hours for CII and 72 hours for other sectors, alongside a graduated classification system for incidents based on severity and corresponding response procedures. The anticipated outcome of this codification is the creation of a unified legal framework that addresses gaps and overlaps, enhances the predictability of regulation, and simplifies compliance for economic actors.

A second critical area of modernisation is the establishment of an effective institutional architecture to coordinate the efforts of different agencies in the field of cybersecurity. By mid-2026, it will be necessary to establish a National Cybersecurity Headquarters within the Office of the Prime Minister, with authority for strategic planning, coordinating the activities of all agencies in cybersecurity, approving mandatory standards for CII, and allocating budgetary resources. The proposed structure should include representatives from the MDDIAI, the Committee for National Security, the Ministry of Internal Affairs, the Ministry of Defence, and the private sector, thereby ensuring interagency coordination and public-private partnership, following the model of Japan's NISC. Concurrently, KZ-CERT should be reorganised into a fully-fledged national incident response centre with expanded powers, an increased staff of up to 100 specialists by 2028, and a budget sufficient to implement early threat detection systems and automated analysis. This approach would eliminate the duplication of functions across agencies, increase the speed of response to cyber incidents by 40%, and improve coordination between the public and private sectors.

A third priority is the strengthening of sanctions mechanisms and the introduction of an objective system for monitoring the effectiveness of law enforcement activities in combating cybercrime. By 2027, amendments should be made to the Criminal Code of the Republic of Kazakhstan No. 226-V KRZ (2014), raising maximum penalties for cybercrimes to levels commensurate with the potential losses arising from such offences. The proposed amendments envisage the introduction of fines for organisations of up to 10,000 MCI or 3% of annual turnover, whichever is higher, custodial sentences of up to seven years for basic offences, and up to 12 years for aggravated offences involving CII, thereby aligning Kazakhstan's legislation more closely with the standards of South Korea and China. Simultaneously, it is necessary to establish mandatory KPIs for law enforcement agencies, including a target of 50% for the proportion of cybercrimes solved by 2028, an average time from detection to suspect apprehension of 30 days for internal affairs cases, and a target of 60% for cases brought to a guilty verdict by 2028. To achieve these targets, specialised cyber-police units should be established in each regional directorate of the Ministry of Internal Affairs, staffed with a minimum of 15 certified specialists who have completed international training in digital forensics. Implementing this package of measures will enhance the preventive effect of criminal

sanctions, increase the proportion of solved cybercrimes from the current 36% to 50%, and strengthen citizen and business confidence in the effectiveness of the law enforcement system.

A fourth strategic priority is the systematic development of human capital in cybersecurity, identified as the weakest link in Kazakhstan's system according to international rankings. By 2027, the Ministry of Education and Science should increase the number of cybersecurity and related programmes to 25 undergraduate and 15 postgraduate courses in leading national universities, representing more than a twofold increase from the current level. In parallel with the expansion of formal education, it is advisable to introduce a state programme for the training and certification of cybersecurity specialists, targeting 5,000 certified professionals by 2028. This would more than triple the current number of approximately 1,500 specialists. To support continuous professional development, a national centre for advanced training should be established for civil servants and employees of CII, with mandatory cybersecurity courses every two years. An additional incentive to attract young talent to the cybersecurity field could be the introduction of scholarship programmes for students in relevant disciplines, with a compulsory service period of at least three years in government bodies or at CII facilities. Comprehensive implementation of these measures will ensure the labour market has sufficient qualified personnel, reduce dependence on foreign consultants, and raise the overall level of cybersecurity awareness across society.

The proposed measures can be applied by the MDDIAI and the State Technical Service to draft a unified cybersecurity law and establish a centralised coordination centre. Strengthening the training of investigators and specialised cyber-police units will contribute to an increased rate of accountability for cybercrime and enhance the overall effectiveness of law enforcement. The findings of this study may also serve as a reference for private-sector entities in developing corporate cybersecurity strategies and provide a model for other Central Asian countries currently modernising their cybersecurity systems.

Discussion

The identified fragmentation of Kazakhstan's cybersecurity legal framework is corroborated by global trends analysed by international researchers. A. Marotta & S. Madnick (2025) examined over 170 cybersecurity regulations across different world regions and identified inconsistencies between national approaches to cyberspace governance. Their study revealed that organisations operating in international environments face a complex web of international, national, and local regulations, complicating compliance due to variations in scope, stringency, and enforcement. These findings align with the situation in Kazakhstan, where the absence of a single codified law and the coexistence of multiple regulatory instruments of varying legal authority reflect similar challenges. Moreover, the study demonstrates that regulatory fragmentation is not limited to transitional economies but is also characteristic of developed jurisdictions, indicating that this is a systemic global challenge.

The observed rise in cyber incidents in Kazakhstan, with an average annual growth rate of 14.5%, mirrors the global escalation of cyber threats, as confirmed by European studies. N. Vandezande (2024) analysed European Union statistics and found that the proportion of enterprises affected by cyber incidents increased from 12% in 2018 to 22% in 2021, reflecting a similar trend in threat growth. The research also recorded a 41% increase in ransomware attacks in 2022 and a 48% rise in email-based attacks, correlating with Kazakhstani data showing the predominance of malware (66% of incidents) and phishing campaigns (20% of incidents). R. Pellreddy (2025) highlights the growing vulnerability of CII to cyber threats, corroborating Kazakhstani data that identify the most frequently targeted sectors: financial services, public administration, telecommunications, and energy. D. Markopoulou & V. Papakonstantinou (2021) analysed the concept of CII in the context of cyber threats and found that the increasing dependence of CII on ICT for operational functionality creates complex challenges for both infrastructure operators and policymakers. This convergence of findings indicates that cybersecurity challenges are universal, irrespective of a country's level of economic development.

The low effectiveness of law enforcement in Kazakhstan, with only 36% of cases reaching prosecution, finds parallels in studies of incident response systems in other jurisdictions. S. Busetti & F.M. Scanni (2025) examined the operation of incident reporting systems in Italy and identified mixed outcomes in their effectiveness. The researchers noted difficulties in detecting and reporting incidents due to organisational capacity constraints, reluctance to report breaches, and limited ability to respond to complex incidents. At the same time, the study shows that even with improvements in reporting system design, from NIS1 to NIS2, the connection between incident reporting and the learning process remains weak due to inertia at both central and local levels. These conclusions align closely with Kazakhstani challenges in pre-trial investigation, the insufficiency of specialised units, and difficulties in identifying perpetrators and collecting digital evidence.

The statistically negative correlation identified between governance quality indicators and the level of cybercrime in Kazakhstan is supported by studies of corporate cybersecurity governance in other countries. W. Tan *et al.* (2025) examined the relationship between corporate cybersecurity governance and the market value of Chinese companies, finding that effective cybersecurity governance enhances trust among investors and suppliers through a reputation-building mechanism. The researchers noted that the reputational effect is particularly pronounced in companies with non-myopic management, stronger protection of trade secrets, and greater media attention to environmental, social, and corporate governance issues. These findings underscore the importance of institutional quality not only

at the state level but also within corporations to ensure effective cybersecurity. E. McCoy (2025) analysed the regulatory landscape of the financial sector in the United States of America, the United Kingdom, and the European Union, highlighting challenges arising from policy inconsistencies across governance levels, which complicate the effective regulation of cybersecurity.

A comparative analysis of the Kazakhstani system against Asian practices revealed fundamental differences in procedural mechanisms and institutional architecture, corroborated by research on the evolution of regional cybersecurity approaches. K. Komiyama (2025) examined Japan's proactive cyber defence reforms and identified the complexities involved in transitioning from a traditionally defensive stance to proactive cybersecurity strategies. The Japanese experience illustrates the critical role of legislative reform in expanding the authority of cybersecurity bodies and establishing centralised coordination among multiple government agencies. D.H. Kim & D.H. Park (2024) compared South Korea's PIPA with the European General Data Protection Regulation and identified shortcomings in the protection of fundamental rights within certain aspects of Korean legislation, reflecting a broader challenge faced by countries harmonising national laws with international standards. J.A. Tagud *et al.* (2024) conducted a comparative analysis of the cybersecurity landscape in Asian countries and revealed disparities in cyber threat preparedness, noting that the Philippines faces challenges similar to Kazakhstan, with moderate cyber vulnerabilities despite legislative improvements.

The identified features of personal data localisation in Kazakhstan contrast with research findings on the risks of rigid localisation for effective cybersecurity. P. Swire *et al.* (2024) analysed the impact of data localisation on the techniques, tactics, and procedures of both cyber threat actors and defenders, establishing that localisation requirements create obstacles to effective cyber defence. The researchers found that halving the number of IP addresses available to defenders more than doubles the time required to detect new attacks, calling into question the effectiveness of Kazakhstan's approach to localisation without corresponding mechanisms for international coordination. R. Su & D. Zhang (2025) examined the evolution of China's transnational data governance strategy, demonstrating that China has developed a multi-level and flexible legal framework that balances sovereign claims with selective openness, reflecting a pragmatic response to domestic needs and international pressures. This approach contrasts sharply with Kazakhstan's fragmented system, which lacks a clear strategic orientation on data localisation.

The analysis of the diversity of national approaches to cybersecurity regulation is supported by studies comparing legal systems across different regions of the world. S. Lim & J. Oh (2025) conducted a comprehensive comparative analysis of privacy legislation in five major regions and identified divergent approaches shaped by unique historical, political, and cultural contexts. They found that the European GDPR emphasises individual rights in response to historical abuses of personal information, the California Consumer Privacy Act (CCPA) prioritises consumer rights within a self-regulatory framework, China's PIPL prioritises national security, Japan's APPI balances individual privacy with societal norms, and South Korea's PIPA combines individual autonomy with a sense of communal responsibility. O.M.T. Kam (2025) compared the European GDPR with China's PIPL, highlighting the importance of clearly defining regulatory powers and noting that the ambiguous authority of China's CAC creates unpredictability in regulatory actions.

The institutional coordination challenges identified in Kazakhstan are echoed in studies of other countries facing similar difficulties in organising effective cybersecurity governance. C. Lötter (2025) analysed South African legislation in comparison with Australian practices and identified deficiencies in national measures without active international coordination. The study highlighted three key lessons from the Australian experience: the establishment of a proactive federal expert group, the criminalisation of ransom payments, and restrictions on the storage of sensitive personal data. M.G. Ali (2025) examined cybersecurity management in higher education institutions and emphasised the need for a comprehensive approach that integrates policy, technology, and organisational culture, a finding that aligns with Kazakhstan's challenges regarding the gap between knowledge and behaviour in cybersecurity. G. Kennedy *et al.* (2025) analysed recent developments in the telecommunications sector in Asian countries and highlighted proactive efforts to strengthen cybersecurity regulation in critical sectors, contrasting with the relative stagnation of Kazakhstan's system.

The findings underscore the importance of adapting international experience to national contexts and reveal the particularities of developing cybersecurity systems in countries with transitional economies. Observed patterns demonstrate the role of institutional quality in effectively ensuring cybersecurity and the necessity of a holistic approach to modernising national cyber defence systems. Comparative analysis with international practices indicates potential avenues for improving Kazakhstan's system by adopting successful elements from Asian models while retaining national regulatory specificities.

Conclusions

This study focused on a comprehensive analysis of Kazakhstan's cybersecurity system through the lens of its legal and regulatory landscape, institutional mechanisms, and empirical performance indicators in comparison with leading practices in East Asia. The multi-faceted analysis identified systemic issues within the national cybersecurity framework and highlighted key areas for modernisation based on international experience. Legal examination of current Kazakhstani legislation revealed a fragmented regulatory system lacking a unified codified act, with the legal foundation comprising two primary legislative acts that do not

include specific provisions for cyber incidents or interagency coordination mechanisms. An analysis of empirical performance indicators revealed a sustained increase in cyber incidents, with an average annual growth rate of 14.5%, a thirty-sixfold rise in registered cybercrimes between 2018 and 2021, and low enforcement effectiveness, with only 36% of registered cases resulting in convictions. A comparative legal analysis of the cybersecurity systems in Japan, South Korea, and China identified key elements of successful national strategies, including the presence of comprehensive framework legislation, the operation of specialised coordinating bodies, mandatory certification systems, and a graduated approach to data protection.

A statistically significant negative correlation was observed between governance quality indicators and levels of cybercrime. Countries with low control-of-corruption scores exhibited, on average, 40% higher cybercrime rates compared with countries with positive scores, indicating a direct relationship between institutional quality and the effectiveness of cyber defence. The study also highlighted fundamental differences in procedural mechanisms, sanctioning measures, and institutional architecture between Kazakhstan's system and leading Asian cybersecurity practices, particularly regarding incident reporting timelines, the magnitude of penalties, and the level of centralisation in coordination functions. A limitation of the study is the lack of publicly available sectoral statistics on financial losses from cybercrime, as well as internal government documents regulating procedures for responding to cyber incidents. A promising direction for further research is a comprehensive analysis of the effectiveness of public-private partnerships in cybersecurity and the development of a methodology for assessing the economic efficiency of investments in the national cyber defence system.

Acknowledgements
None.

Funding
None.

Author Contributions
G. Ismailova conceived and supervised the study and drafted the manuscript. N. Kadirova conducted data collection and analysis and contributed to the methodology. Both authors revised the manuscript and approved the final version.

Conflict of Interest
None.

References
[1] Abuova, N. (2024). Kazakhstan advances in global cybersecurity index 2024. *The Astana Times*. Retrieved from https://astanatimes.com/2024/09/kazakhstan-advances-in-global-cybersecurity-index-2024/.
[2] Act of Japan No. 104 "The Basic Act on Cybersecurity". (2014, November). Retrieved from https://www.japaneselawtranslation.go.jp/en/laws/view/3677/en.
[3] Act of Japan No. 128 "Act on Prohibition of Unauthorized Computer Access". (1999, August). Retrieved from https://www.japaneselawtranslation.go.jp/en/laws/view/3933/en.
[4] Act of Japan No. 57 "Act on the Protection of Personal Information". (2003, May). Retrieved from https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en.
[5] Act of the Republic of Korea No. 14080 "Act on Promotion of Information and Communications Network Utilization and Information Protection". (2016, March). Retrieved from https://elaw.klri.re.kr/eng_service/lawView.do?hseq=38422&lang=ENG.
[6] Act of the Republic of Korea No. 14122 "Credit Information Use and Protection Act". (2016, March). Retrieved from https://law.go.kr/LSW/lsInfoP.do?lsiSeq=182111&urlMode=engLsInfoR&viewCls=engLsInfoR#0000.
[7] Act of the Republic of Korea No. 19234 "Personal Information Protection Act". (2023, March). Retrieved from https://elaw.klri.re.kr/eng_service/lawView.do?hseq=62389&lang=ENG.
[8] AEQUITAS Law Firm. (2024). *Doing business in Kazakhstan: Legal basics*. Retrieved from https://aequitas.kz/upload/files/2024/AE_Doing%20Business%202024%20(Eng).pdf.
[9] Akhmetova, S. (2024). *Personal data protection, state oversight and legislative updates*. Retrieved from https://www.mondaq.com/data-protection/1474888/personal-data-protection-state-oversight-and-legislative-updates.
[10] Al-Farabi Kazakh National University. (n.d.). *Criminal offenses in the field of informatization and communication (criminal law and criminological aspects)*. Retrieved from https://old.abu.edu.kz/uploads/182/791/1089/89b592eca7a3f879eeeb8e258c189ab5.pdf.
[11] Ali, M.G. (2025). *Cybersecurity governance and policy development in higher education institutions: A strategic framework for resilience and compliance*. Retrieved from https://files.eric.ed.gov/fulltext/ED675147.pdf.
[12] Amirov, A., Kainazarova, D., Begaliyev, E., Sarsenbaev, A., & Kurbanbaev, N. (2024). Legal ways and methods of personal data protection in Kazakhstan. *Scientific Herald of Uzhhorod University, Series "Physics"*, 55, 2174-2186. doi: 10.54919/physics/55.2024.217wl4.
[13] Anderson, C., Crete-Nishihata, M., Dehghanpoor, C., Deibert, R., McKune, S., Ottenheimer, D., & Scott-Railton, J. (2015). *Are the kids alright? Digital risks to minors from South Korea's smart sheriff application*. Retrieved from https://citizenlab.ca/2015/09/digital-risks-south-korea-smart-sheriff/.

[14] APCERT. (2024). *APCERT Annual Report 2024*. Retrieved from https://www.apcert.org/documents/pdf/APCERT_Annual_Report_2024.pdf.
[15] Baker McKenzie. (2025). *Global data and cyber handbook: South Korea*. Retrieved from https://resourcehub.bakermckenzie.com/en/resources/global-data-and-cyber-handbook/asia-pacific/south-korea/topics/key-data-and-cybersecurity-laws.
[16] Busetti, S., & Scanni, F.M. (2025). Evaluating incident reporting in cybersecurity. From threat detection to policy learning. *Government Information Quarterly*, 42(1), article number 102000. doi: 10.1016/j.giq.2024.102000.
[17] Cho, S. (2022). National cybersecurity organisation: Republic of Korea. In *National cybersecurity governance series* (pp. 1-27). Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.
[18] Code of the Republic of Kazakhstan No. 235-V KRK "On Administrative Infractions". (2014, July). Retrieved from https://adilet.zan.kz/kaz/docs/K1400000235.
[19] Committee for National Security of the Republic of Kazakhstan. (2021). *On the prevention of a cyberattack*. Retrieved from https://www.gov.kz/memleket/entities/knb/press/news/details/145642.
[20] Committee of National Security of the Republic of Kazakhstan. (2025). *About the court sentence*. Retrieved from https://www.gov.kz/memleket/entities/knb/press/news/details/934421.
[21] Council of Europe. (2022). *Second additional protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224)*. Retrieved from https://www.coe.int/en/web/cybercrime/second-additional-protocol/-/asset_publisher/isHU0Xq21lhu/content/opening-coecyber2ap.
[22] Council of Europe. (2023). *Kazakhstan invited to join the Convention on Cybercrime*. Retrieved from https://www.coe.int/en/web/portal/-/kazakhstan-invited-to-join-the-convention-on-cybercrime.
[23] Council of Europe. (2024). *Octopus project: Authorities of Kazakhstan coordinate on the next steps to complete accession to the Convention on Cybercrime*. Retrieved from https://www.coe.int/en/web/cybercrime/-/octopus-project-authorities-of-kazakhstan-coordinate-on-the-next-steps-to-complete-accession-to-the-convention-on-cybercrime.
[24] Creemers, R., Webster, G., & Triolo, P. (2018). *Cybersecurity Law of the People's Republic of China*. Retrieved from https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.
[25] Criminal Code of the Republic of Kazakhstan No. 226-V KRZ. (2014, July). Retrieved from https://adilet.zan.kz/kaz/docs/K1400000226.
[26] Criminal Law of the People's Republic of China. (1979, July). Retrieved from https://english.court.gov.cn/2015-12/01/c_761557.htm.
[27] Criminal Procedure Code of the Republic of Kazakhstan No. 231-V KRZ. (2014, July). Retrieved from https://adilet.zan.kz/eng/docs/K1400000231.
[28] Cyber attacks of 2024: How to protect yourself in the age of digital threats. (2025). *State technical service*. Retrieved from https://sts.kz/en/news/066a2c46-3ce0-4aea-b97d-76733d6b8b0b.
[29] Eurasian Research Institute. (2025). Digital security and threats in Kazakhstan. *E-Bulletin Analysis*, 376.
[30] Forum of Incident Response and Security Teams. (n.d.). *KZ-CERT team information*. Retrieved from https://first.org/members/teams/kz-cert.
[31] Global Cybercrime Report 2024: Which countries face the highest risk? (2024). *MixMode threat research*. Retrieved from https://mixmode.ai/blog/global-cybercrime-report-2024-which-countries-face-the-highest-risk/.
[32] Government Decree of the Republic of Kazakhstan No. 269 "Concept for Digital Transformation, Development of Information and Communication Technologies and Cybersecurity Industry for 2023-2029". (2023, May). Retrieved from https://adilet.zan.kz/kaz/docs/P2300000269.
[33] Government Decree of the Republic of Kazakhstan No. 407 "Concept on Cybersecurity (Kazakhstan's Cyber Shield)". (2017, June). Retrieved from https://adilet.zan.kz/kaz/docs/P1700000407.
[34] Government of Japan. (n.d.). Retrieved from https://www.nisc.go.jp/eng/pdf/cip_policy_2024_eng.pdf.
[35] Greenleaf, G., & Kaldani, T. (2025). Data privacy laws in Central Asia: Between ex-SSR and 'Belt & Road'. *International Data Privacy Law*, 15(1), 67-90. doi: 10.1093/idpl/ipae015.
[36] Hernandez, J.R. (n.d.). *What is the actual cost of cybercrime?* Retrieved from https://evolvesecurity.com/blog-posts/actual-cost-of-cybercrime.
[37] International Telecommunication Union. (2020). *Global cybersecurity index 2020*. Geneva: ITU Publications.
[38] International treaty UK/Kazakhstan TS No.25/2016 "Treaty on Mutual Legal Assistance in Criminal Matters". (2016, April). Retrieved from https://www.state.gov/wp-content/uploads/2019/02/16-1206-Kazakhstan-Law-Enforcmt-MLAT.pdf.
[39] Japan Computer Emergency Response Team Coordination Center. (n.d.). *About JPCERT/CC*. Retrieved from https://jpcert.or.jp/english/about/.
[40] JPCERT Coordination Center. (2024). *JPCERT/CC Incident Handling Report: January 1, 2024 - March 31, 2024*. Retrieved from https://jpcert.or.jp/english/doc/IR_Report2023Q4_en.pdf.

[41] Kam, O.M.-T. (2025). A comparative analysis of customer data privacy protection under the European Union's general data protection regulation and the People's Republic of China's personal information protection law. *Beijing Law Review*, 16(3), article number 163086. doi: 10.4236/blr.2025.163086.
[42] Katagiri, N. (2022). Assessing Japan's cybersecurity policy: Change and continuity from 2017 to 2020. *Journal of Cyber Policy*, 7(1), 38-54. doi: 10.1080/23738871.2022.2033805.
[43] Kennedy, G., *et al.* (2025). Asia-pacific developments. *Computer Law & Security Review*, 57, article number 106151. doi: 10.1016/j.clsr.2025.106151.
[44] Kergroach, S., Becker, S., & Bernat, L. (2024). *Shielding SMEs – how to boost their defence against cyberattacks*. Retrieved from https://oecdcogito.blog/2024/04/03/shielding-smes-how-to-boost-their-defence-against-cyberattacks-2/.
[45] Kim, D.H., & Park, D.H. (2024). Automated decision-making in South Korea: A critical review of the revised personal information protection act. *Humanities and Social Sciences Communications*, 11, article number 974. doi: 10.1057/s41599-024-03470-y.
[46] Komiyama, K. (2025). Norms in new technological domains: What's next for Japan and the United States in cyberspace. In *Strategic Japan* (pp. 1-8). Washington, DC: Center for Strategic and International Studies (CSIS).
[47] Kubanova, N., Neselbayeva, I., Dyussebalyeva, S., Halibati, H., & Adilgazy, S. (2024). Countering cyber attacks in the Republic of Kazakhstan: Interdisciplinary issues and legal frameworks in the context of social security and economic stability. *Social & Legal Studies*, 8(1), 179-194. doi: 10.32518/sals1.2025.179.
[48] Kubanova, N.B. (2025). Forensic characterization of cyber attacks. *Bulletin of Institute of Legislation and Legal Information of the Republic of Kazakhstan*, 80(2), 278-288. doi: 10.52026/2788-5291_2025_80_2_278.
[49] Kulzhabayeva, Z.O. (2024). Legislative distinction between the concepts of "cybersecurity" and "information security". *Scientific and Legal Journal "Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan"*, 4(79), 178-184. doi: 10.52026/2788-5291_2024_79_4_178.
[50] Law of the People's Republic of China No. 84 "Data Security Law of the People's Republic of China". (2021, June). Retrieved from https://en.npc.gov.cn.cdurl.cn/2021-06/10/c_689311.html.
[51] Law of the People's Republic of China No. 91 "Personal Information Protection Law of the People's Republic of China". (2021, August). Retrieved from https://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.html.
[52] Law of the Republic of Kazakhstan No. 418-V ZRK "On Informatization". (2015, November). Retrieved from https://adilet.zan.kz/kaz/docs/Z1500000418.
[53] Law of the Republic of Kazakhstan No. 94-V ZRK "On Personal Data and Their Protection". (2013, May). Retrieved from https://adilet.zan.kz/kaz/docs/Z1300000094.
[54] Less than half of criminal cases on cybercrimes in 2024 reached court in Kazakhstan. (2025). *Kazakh telegraph agency*. Retrieved from https://surl.li/ypluff.
[55] Lim, S., & Oh, J. (2025). Navigating privacy: A global comparative analysis of data protection laws. *IET Information Security*, 2025(1), article number 5536763. doi: 10.1049/ise2.5536763.
[56] Lötter, C. (2025). A comparative critique of the Cybercrimes Act 19 of 2020: Positioning South Africa vis-à-vis Australia. *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad*, 28(1), 1-33. doi: 10.17159/1727-3781/2025/v28i0a17035.
[57] Markopoulou, D., & Papakonstantinou, V. (2021). The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular. *Computer Law & Security Review*, 41, article number 105502. doi: 10.1016/j.clsr.2020.105502.
[58] Marotta, A., & Madnick, S. (2025). Analyzing and categorizing emerging cybersecurity regulations. *ACM Computing Surveys*, 58(2), 1-36. doi: 10.1145/3757318.
[59] McCoy, E. (2025). Cybersecurity regulations and risk management in the financial sector: A comparative analysis. *Law Economics and Society*, 1(1), 115-135. doi: 10.30560/les.v1n1p115.
[60] Mukhametgali, F. (2024). *Kostanay resident convicted for distributing malicious software on the internet*. Retrieved from https://polisia.kz/ru/kostanajtsa-osudili-za-rasprostranenie-v-internete-vredonosnoj-programmy/.
[61] National Cyber Security Index. (n.d.). *Kazakhstan*. Retrieved from https://ncsi.ega.ee/country/kz/.
[62] Nguyen, T.A., Koblandin, K., Suleymanova, S., & Volokh, V. (2021). Effects of 'digital' country's information security on political stability. *Journal of Cyber Security and Mobility*, 11(1), 29-52. doi: 10.13052/jcsm2245-1439.1112.
[63] Orumbayeva, M., & Kurmangali, A. (2022). Cybersecurity and current global threats in Central Asia. *Memlekettik Basqaru zhane Memlekettik Qyzmet*, 2(81), 77-84. doi: 10.52123/1994-2370-2022-657.
[64] Pellreddy, R. (2025). Cybersecurity for critical infrastructure: Protecting national assets in the digital age. *International Journal of Computer Trends and Technology*, 73(2), 7-17. doi: 10.14445/22312803/IJCTT-V73I2P102.
[65] Personal Information Protection Commission. (2022). *Guidelines for Act on the Protection of Personal Information*. Retrieved from https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/.
[66] Regulations on the Management of Online Data Security (Draft for Solicitation of Comments). (2021). Retrieved from https://www.chinalawtranslate.com/en/data-security-management-draft/.

[67] South Korea's 2024 Cyber Strategy: A Primer. (2024). Retrieved from https://csis.org/blogs/strategic-technologies-blog/south-koreas-2024-cyber-strategy-primer.
[68] Stickings, M., & Nosal., J. (2024). *Blunting the cutting edge of crime: OSCE helps combat cybercrime in Central Asia*. Retrieved from https://osce.org/blog/574757.
[69] Su, R., & Zhang, D. (2025). Adaptive sovereignty: China's evolving legislative framework for transnational data governance. *Politics and Governance*, 13, article number 10413. doi: 10.17645/pag.10413.
[70] Swire, P., Kennedy-Mayo, D., Bagley, D., Krasser, S., Modak, A., & Bausewein, C. (2024). Risks to cybersecurity from data localization, organized by techniques, tactics and procedures. *Journal of Cyber Policy*, 9(1), 20-51. doi: 10.1080/23738871.2024.2384724.
[71] Syrlybayeva, F., Kassymova, X., Omarova, E., Zhussipova, B., & Nurgalieva, E. (2024). Protection of information about employee's personal data in the Republic of Kazakhstan. *Social & Legal Studies*, 7(4), 90-102. doi: 10.32518/sals4.2024.90.
[72] Tagud, J.A., Gildo, E., Jabay, U.A., Oro, E., Sagaldia, S.M., & Tigtig, R.F. (2024). Comparative analysis of the cybersecurity landscape in Asian countries using linear regression. *SAR Journal*, 7(4), 404-410. doi: 10.18421/SAR74-15.
[73] Tan, W., Guo, B., & Zhang, Q. (2025). Cybersecurity governance and corporate market value: Perspectives from investor trust and supply chain trust. *Pacific-Basin Finance Journal*, 90, article number 102646. doi: 10.1016/j.pacfin.2024.102646.
[74] Univision.kz. (n.d.a). *B058 information security*. Retrieved from https://univision.kz/edu-program/group/B058-informatsionnaya-bezopasnost.html.
[75] Univision.kz. (n.d.b). *M095 information security*. Retrieved from https://univision.kz/edu-program/group/M095-informatsionnaya-bezopasnost.html.
[76] Vandezande, N. (2024). Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. *Computer Law & Security Review*, 52, article number 105890. doi: 10.1016/j.clsr.2023.105890.
[77] Worldwide Governance Indicators. (2024). *World Bank Group*. Retrieved from https://databank.worldbank.org/reports.aspx?Id=ceea4d8b&Report_Name=WGI-Table.
[78] Zhamburbayeva, S., & Ilsasova, G.A. (2024). The realization of the "Concept of digital transformation, development of the information and communication technologies and cybersecurity industry for 2023-2029" by implementing blockchain technologies of the Republic of Kazakhstan and the problems of its legal regulation. *Bulletin of the Karaganda University*, 4(116), 137-146.
[79] Zhang, C. (2024). China's privacy protection strategy and its geopolitical implications. *Asian Review of Political Economy*, 3, article number 6. doi: 10.1007/s44216-024-00028-2.