Journal of Posthumanism

2025
Volume: 5, No: 5, pp. 965–979
ISSN: 2634-3576 (Print) | ISSN 2634-3584 (Online)
posthumanism.co.uk

DOI: https://doi.org/10.63332/joph.v5i5.1415

China's Co-Operation with Central Asian Countries on Cyber Security

Sarybayev Mura[1], Kaliyeva Yeleukhan[2], Zhekenov Duman[3], Islambek Parkhatzhan[4]

Abstract

The issue of cyber security is becoming more and more important today, so this factor must be taken into account by all governments, because threats in the field of information technology are no less important than threats in any other sphere of state activity. So, cybersecurity is the state or process of protecting and recovering computer systems, networks, devices and programmes from any type of cyberattack. Cyberattacks pose an increasingly sophisticated and growing threat to sensitive user data worldwide as attackers use new techniques based on social engineering and artificial intelligence to circumvent traditional data security controls. It is worth noting that the modern world is increasingly reliant on computer technology, and this reliance will only increase over time. In particular, this is fuelled by a generation of new technologies that will access our connected devices via Bluetooth and Wi-Fi, making it easier for attackers to commit illegal acts.

Introduction

Thus, it can be said that the importance of cybersecurity in today's world is growing rapidly. In general, as of today, our society is more technologically dependent than ever before, and there is no indication that this trend will slow down. In addition, sensitive information such as national insurance numbers, credit card details and bank account details are now stored on cloud storage services such as Dropbox or Google Drive, which also makes it easier for these data to be stolen [1].

Whether an entity is an individual, a small business or a large multinational company, it always relies on computer systems [2]. Realising this and recalling the above fact about the strengthening of cloud storage. It can also be noted that the issue of personal data protection is one of the most urgent in the modern world.

Note the difference between the terms information security and cybersecurity. The former is used to refer to data protection, while the latter is more broadly defined, as it includes this aspect and the creation and debugging of software. Thus, the concept of information security is more characteristic in the context of forming a culture of information technology use by individual users, and cybersecurity is a branch of professionals whose goal is to create a secure information environment [3]. In this regard, cybersecurity is the object of consideration of this section of this research paper.

[1] Al-Farabi Kazakh national university, Almaty, Kazakhstan, Email: tokhtarsenbekuli@gmail.com
[2] Al-Farabi Kazakh national university, Almaty, Kazakhstan
[3] Al-Farabi Kazakh national university, Almaty, Kazakhstan.
[4] Almaty Academy of the Ministry of International Affairs named after Makan Yesbulatov, Almaty, Kazakhstan.

There is a need to consider the effects that cybercrime can have on society. In particular, this may apply to the lives of individual citizens, as cybercriminals can steal personal information such as names, e-mail addresses, telephone numbers, passwords and financial data. This information can be used for fraud, identity theft and other crimes. In addition, cybercriminals can create and distribute malware, particularly viruses. These applications can be used to steal information, corrupt files and systems, or for ransomware.

On a national scale, cybercrime can cause significant damage and create the conditions to rock the security situation in a particular country. This can be accomplished in a variety of ways, depending on the goals and objectives of the operation. One example of this is cyber attacks on critical infrastructure. Such actions can lead to destruction and disruption of law and order in various spheres of life. It is worth noting that critical infrastructure includes energy networks, water supply, transport, banking and financial systems, telecommunications networks and other systems vital to the functioning of a country. All of the above infrastructure can be attacked by cybercriminals [4].

Attacks on critical infrastructure can be carried out for various motives such as ransomware, espionage, military purposes and terrorism. Cyberattacks can be carried out through various methods such as viruses, various programmes, DDoS attacks that involve disabling Internet resources by overloading them, and other methods [2].

Materials and Methods

The consequences of cyber attacks on critical infrastructure can be quite severe. For example, an attack on the electrical grid can lead to power outages and disruption of many systems, which can cause significant economic and social disruption. On the other hand, attacks on banking and financial systems can lead to theft of funds, as well as disruption of the financial system [5].

Another threat to the activities of cybercriminals is the theft of sensitive government information. In the context of addressing this issue, it is necessary to define this basic concept. Confidential state information is information that contains state secrets, i.e. information that is not subject to disclosure or free access. State secrets are information relating to national security, state sovereignty, economic interests of the state, foreign policy relations, defence, and state secrets. In general, such information is characterised by the fact that it is contained in documents designated as ‘for official use only’, ‘of special importance’, ‘secret’ and others. Confidential state information can be stored in various formats, including electronic files, databases and others [6].

Also, sensitive State information may contain important military, political, economic and diplomatic documents that could be used against the State, the theft of which could have significant national security implications. For example, information on defence plans, armed forces and military technology may be shared with other countries or terrorist organisations, which could have serious consequences for the security of the State [6].

In addition, sensitive information may contain important national security details, such as information about critical infrastructure, energy systems and other critical facilities that could be used against the state [7]. Thus, the theft of such information can lead to serious consequences such as terrorist attacks and other acts of violence.

The theft of sensitive government information can also have serious economic consequences. In particular, information about important economic plans, technology and intellectual property

may be transferred to other countries or companies, which may create an unequal playing field for businesses in the relevant industry. This can lead to reduced revenues and job losses, which in turn can affect the economic stability of the state [8].

Also, important confidential information about financial, trade agreements and other important economic documents can be used for improper gain. For example, the ability to specify the terms of a trade agreement or to commit financial fraud can have serious consequences for a state's economy.

The theft of confidential government information can also lead to a breach of trust in government agencies and institutions. Citizens and other states may lose confidence in authorities and public bodies that have failed to protect confidential information [9]. This can have serious consequences for the sustainability of public institutions and their management of the state.

In addition, the theft of sensitive government information can have serious consequences for international security. If the information is shared with other countries, it can lead to increased tension between States, as well as increased conflict and strained international relations [10]. In addition, confidential State information can be used to commit terrorist acts and other forms of violence, which can jeopardise the security of individuals and States.

In general, the theft of sensitive government information is a serious problem that can have significant consequences for the state and its citizens. It can lead to loss of competitive advantage, reduced revenues and job losses, breach of trust in government agencies and institutions, and a threat to international security. The State must therefore pay particular attention to the protection of confidential information and take the necessary measures to ensure its security and confidentiality.

Examples of serious cybercrime in today's world include the cyberattack on the U.S. government that occurred in December 2020, when hackers infiltrated the systems of the Pentagon, the Treasury Department, and other government agencies. This attack was attributed to a group of hackers linked to Russia [11]. In the same year, there was a cyberattack on the Indian Parliament linked to a Chinese hacker group. The hackers were able to break electronic voting systems and steal sensitive information [12]. Also in December 2017, hackers managed to infiltrate the German government's system and steal sensitive information, including correspondence between government leaders [13].

To understand the impact of cybercrime on the global community, the following statistics should be analysed:

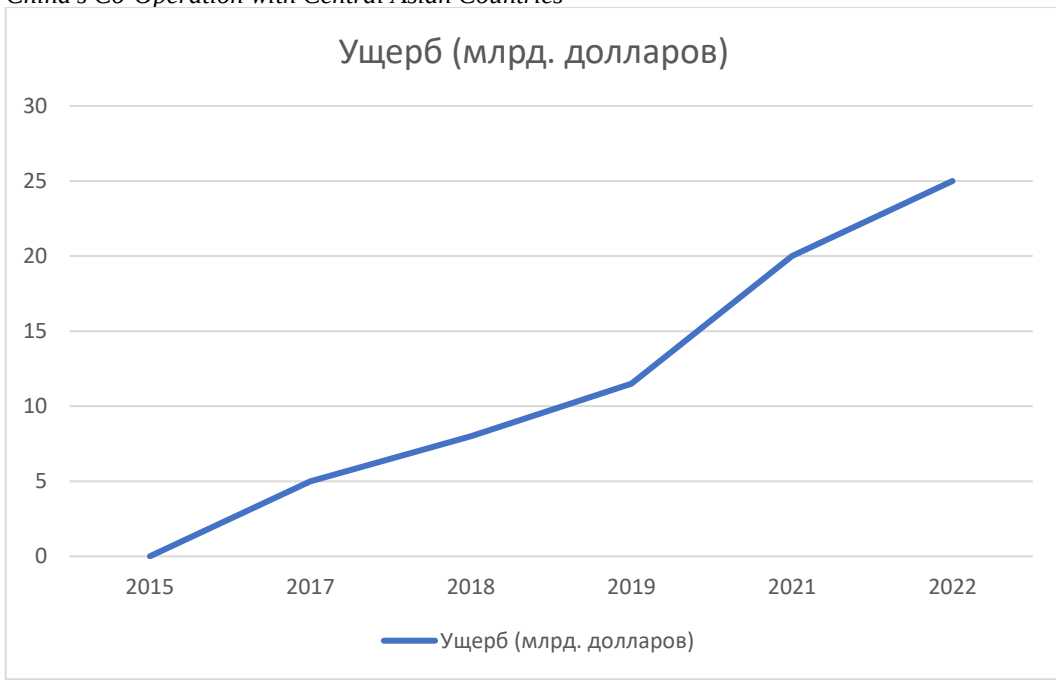

Figure 6: Total Global Damage from Cyberattacks (Billion Dollars)

Source: [14]

It should be noted that the years covered in this infographic correspond to certain socio-political events in the world. In particular, 2015 can be considered as a starting point, as cybercrime starts to gain significant momentum at this time. The data from 2017, 2018 and 2019 are quite revealing, as a gradual increase in the rate of losses from cybercriminals can be observed during this period. In the year 2021, a sharp increase in the said indicator can be observed. The reason for this may be the coronavirus pandemic, as this event was one of the determining factors that contributed to the increase in the use of computer technology worldwide. Also, an increase in global losses can be observed in 2022, which is due to the war in Ukraine.

Results

To summarise, cyber terrorism poses a serious threat to national security as the modern world becomes increasingly dependent on information technology. The Internet and computer networks are used in all areas of life, including the management of energy systems, transport, financial transactions, communications and other critical infrastructures.

As a next step, it is important to consider in more detail how cybercrime is evolving in China and Central Asian countries so that key issues in this area can be understood and possible options for co-operation can be foreseen.

The first cases of computer crime in China began to appear in the mid-1980s, when the first victims of insider computer crime were banking systems [15].

The Internet in China became commercially available in 1995, and since then it has grown rapidly. Various forms of cybercrime have followed. In particular, hacking was the first, leading to the emergence of the Green Army hacker group in 1997, which later gave way to the Red

Hacker Alliance, a loosely connected group of individuals that emerged after the 1998 Jakarta riots, when Chinese citizens were blamed for destabilising. Countries [15].

Since then, Chinese hackers began to actively attack IP addresses within their own country in order to gain profit through illicit enrichment. It is worth noting that since the very beginning of the 21st century, patriotism has not been prevalent among Chinese hackers, causing them to frequently attack their own fellow citizens [15].

Chinese officials first expressed public concern about cybercrime against their citizens in 2001 [16]. In the following years, cybercrime spread further due to a lack of sufficient defences as well as economic changes.

In addition, the rise in unemployment in the mid-2000s led to a large number of young unemployed people trying to fulfil themselves in cybercrime. The wave of online crime began to spread to different industries and even to smaller and distant cities. In some of them, phishing (obtaining personal user data) and other cybercrimes began to supplant traditional crimes. Most hackers were technologically inexperienced, buying off-the-shelf hacking tools from professional hackers overseas. With this in mind, Chinese law enforcement focused on shutting down online marketplaces where these tools were sold, but with mixed success [16].

Since then, hackers have become more sophisticated in their activities, but cybercrime has increasingly spread from simple phishing (as an offence against individuals) to attacks on financial institutions [16]. In response, Chinese officials shut down some of the largest online marketplaces and training sites, but cybercrime still increased dramatically.

In 2008, China's Ministry of Industry and Information Technology reported that 1.2 million Chinese computers had been infected with software that allowed attackers to control them as part of a botnet (a network of compromised computers that a hacker can control remotely without the owner's permission). This has made China a safe haven for about 60 per cent of all the world's computers infected in this way. Given the significant number of computers involved in botnets, China's role as the main culprit of cyberattacks can be explained [17]. Thus, although the botnets could have been controlled by cybercriminals from anywhere in the world, it would seem to the victims that the attacks originated from China. On the other hand, a 2009 government report claimed economic losses of 7.6 billion yuan (US$1.2 billion) [18].

In the second decade of the twenty-first century, cyber attacks grew rapidly. In particular, one such attack forced the Hong Kong Stock Exchange to temporarily suspend trading of seven major companies in 2011. Trading systems were not broken then, but investors were temporarily blocked from receiving important messages scheduled to be published by these companies [19]. In 2015, Hong Kong-based toy company Vtech, was attacked in 2015, exposing the personal information of 4.9 million adult customers and their 6.4 million children [20]. In 2017, a cyberattack called WannaCry was able to encrypt data on the computers of thousands of companies around the world, including Chinese companies and government organisations [21]. In 2018, Chinese bank Ping An Insurance was compromised by a hacker group demanding a ransom in the form of cryptocurrency. However, the bank did not respond to the attackers' demands and fortunately no data was lost [22]. In 2019, several Chinese universities were attacked by attackers who used malware to gain access to sensitive information [23]. This attack resulted in the loss of tens of thousands of students‘ and faculty members’ data.

The history of cybercrime in Central Asia is linked to the growing use of the Internet and information technology in the region. The first Internet service provider appeared in Kazakhstan

in 1995, and in Uzbekistan and Kyrgyzstan in 1997. At the same time, the development of the Internet and computer technology led to an increase in cybercrime in the region [24].

It is worth noting that several cases of cyber attacks on government websites, banks and other organisations were registered in Central Asia in the 2000s. In 2002, the website of the Ministry of Information was broken in Kyrgyzstan, and in 2003, the website of the country's President was broken. Also in 2003, a cyberattack on the banking system in Kazakhstan resulted in the theft of more than $1 million. In the following years, cybercrime in Central Asia continued to grow. In 2007, cases of Internet fraud were recorded in Kazakhstan, when cybercriminals used phishing attacks to steal bank data and money from accounts. At the same time, cybercriminals used social media and other platforms to spread false information, leading to tensions in political and social situations. In the 2010s, cybercrime in Central Asia continued to grow, but criminals began to use more sophisticated and technologically advanced methods [24]. 24] In 2011, a cyberattack on an e-mail network in Kazakhstan resulted in the theft of more than 3 million user e-mails. 25] In 2013, the website of the Ministry of Foreign Affairs in Uzbekistan was broken, and in 2014, the website of the Kyrgyz government was broken.

During the same period, cybercriminals began to actively use cryptocurrencies to commit criminal acts. In 2017, the website of a local cryptocurrency exchange in Tajikistan was broken, resulting in the theft of more than $2 million in cryptocurrencies. At the same time, criminals continued to use phishing attacks and other methods to steal bank data and money from accounts [26].

In addition, cybercrime groups have emerged in Central Asia and are being used to hijack data and money. For example, in 2019, bank websites in Kazakhstan and Uzbekistan were broken using software created by cybercrime groups. In these cases, criminals used social engineering, phishing attacks and other methods to gain access to banking systems and steal money [26].

It is important to note that the criminal cyber group Cobalt has established itself in Kazakhstan due to the lack of proper cyber security development. According to representatives of CARCA's Cyberattack Analysis and Research Centre, Kazakhstani security experts noticed an increase in the number of home computers taken over by Cobalt malware in 2015. They point to the use of broken Kazakhstani servers in the 2016 attack on Bangladesh Bank, when the attack resulted in $81 million in losses. 27] This evidence suggests that the criminal group is based in Central Asia.

Since early 2013, Cobalt has been one of the world's most dangerous hacker groups specialising in breaking into banks. The group initially targeted Russian banks, attacking them with phishing emails. These emails contained programmes that allowed them to access password-protected archives, which in turn gave them remote access to ATMs, which then delivered cash to waiting accomplices. Since 2017, the group has branched out from Eastern Europe and Southeast Asia into Europe and North America. Specifically, according to Europol, Cobalt attacked banks in 40 countries and caused more than $1.1 billion in damage [28].

In addition, cybercrime poses a significant risk to banking and financial institutions in Central Asia, as the lack of knowledge, expertise and defence procedural training among employees makes them vulnerable to attacks such as those mentioned above.

Thus, given that cybercrime poses grave threats in the modern world, much attention is being paid to the development and implementation of cyber defence legislation to effectively combat

cybercrime. One of the largest and most developed regions of the world in terms of cyber legislation is the European Union (EU).

The European Union has considerable experience in combating cybercrime and setting standards for information protection. EU legislation ensures that minimum standards of cyber defence are set, regulating the use of the Internet, data protection, protection of personal data and punishment for cybercrime.

The first cybersecurity legislation adopted by the European Union (EU) is the Network and Information Systems Security Directive (NIS Directive). The Directive was adopted on 6 July 2016 and aims to achieve a high common standard of network and information security across all EU member states. The Directive came into force in August 2016, from which point EU member states have 21 months to integrate its requirements into their own national laws, and a further 6 months to define the companies subject to compliance with the NIS Directive [29].

The NIS sets out a number of network and information security requirements applicable to operators of essential services and digital service providers (DSPs) [29]. In particular, the 'Essential Service Operators' referred to in the legislation include entities in the sectors of energy, transport, banking, financial market infrastructure, healthcare, drinking water supply and distribution, and digital infrastructure. The NIS Directive requires each EU Member State to compile a list of organisations in these sectors that they consider to be essential service providers.

The Directive defines a digital service as 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of the service recipient'. Specific types of DSPs described in the Directive include cloud service providers, online marketplaces and search engines. DSPs should be aware that the NIS Directive also applies to non-EU companies whose services are available in the EU. These companies are required to appoint a representative in the EU to act on their behalf to ensure compliance with the NIS Directive [29]. However, DSPs are subject to a less stringent framework than the 'operators of essential services' set out in the Directive.

The NIS Directive contains a number of requirements for incident response and the implementation of risk-based technical security measures [29]. For example, the requirements aim to improve cross-border co-operation on information and network security and to promote a culture of risk management.

In particular, to improve cross-border co-operation, the Directive will establish a network of Computer Security Incident Response Teams (CSIRTs) in each Member State. Member States must also designate National Competent Authorities (NCAs) and Single Points of Contact (SPoCs) for cybersecurity monitoring, reporting, incident response and other cross-border coordination. CSIRTs must also have access to 'adequate resources and equipment,' including secure and resilient infrastructure. The CSIRT from each member state will have a number of tasks, including monitoring national security incidents, disseminating early warnings, alerts, and cybersecurity announcements, providing dynamic risk analyses, and coordinating with CSIRTs from other member states [29].

In addition, member states must introduce a national cybersecurity strategy that defines security objectives and the relevant policies and regulations necessary to ensure the strategy is implemented. The directive requires that any strategy include such things as a governance structure, response and recovery measures, planning for public-private security cooperation, security education programmes, risk assessment plans, and lists of people and organisations

involved in the strategy. Member States are also required to designate at least one representative to monitor the impact and implementation of the NIS Directive at national level. Each SPoC Member State should communicate with other SPoC Member States to improve co-operation.

In addition, the directive provides for the establishment of a co-operation group whose purpose is to promote co-operation on cybersecurity among member states. The co-operation group consists of representatives of the Member States and the European Union Agency for Network and Information Security (ENISA), with a member of the European Commission acting as the Secretariat. The Co-operation Group focuses on planning, managing and repositioning the implementation of the NIS Directive. The Group's main responsibilities include providing guidance for the new CSIRT network, helping Member States to determine which services should be categorised as 'essential service operators', liaising with relevant authorities on security incidents and issues, sharing security best practices, and generally raising awareness of cybersecurity in the EU. The group is also required to submit a report every 18 months with some detail on the level of co-operation taking place and the progress of implementation of the NIS Directive.

Also, organizations that qualify as DSPs under the criteria of the Directive must implement a range of risk management measures, both technical and operational. DSP organizations must comply with the Directive's incident reporting protocol, which requires organizations to report "without undue delay" to the CSIRT and other relevant authorities any significant security incidents.

However, while the NIS Regulation is a significant step in securing networks and information in Europe, it still falls short of addressing all new cyber threats and challenges. In particular, the Regulation does not take into account emerging technologies such as artificial intelligence and their impact on cybersecurity. In addition, many organizations in Europe still have a low level of cyber protection, so cybersecurity measures need to be further developed and made more effective.

Another important aspect of the Regulation is the creation of the European Cyber Defense Agency (ENISA) [30], which was already established in 2004 and is a key player in information technology security in Europe. ENISA is responsible for developing and disseminating cyber defense recommendations, promoting the development of standards and technologies, and supporting national cyber defense authorities.

Another regulation is the General Data Protection Regulation (GDPR) is the strictest privacy and security law in the world [31]. Although it was developed and adopted by the European Union (EU), it imposes obligations on organizations anywhere as long as they target or collect data related to people in the EU. The regulation went into effect on May 25, 2018. GDPR levies strict fines on those who violate its privacy and security standards, fines will reach tens of millions of euros.

With GDPR, Europe is demonstrating its strong stance on data privacy and security at a time when more and more people are entrusting their personal data to cloud services and breaches are an everyday occurrence. The regulation itself is sweeping, wide-ranging and fairly light on specifics, making GDPR compliance a daunting prospect, especially for small and medium-sized enterprises (SMEs).

The reasons for this regulation are quite profound, because the right to privacy is part of the European Convention on Human Rights of 1950, which says: "Everyone has the right to respect

for his private and family life, his home and his correspondence". On this basis, the European Union has tried to ensure the protection of this right through legislation [32].

As technology evolved and the Internet was invented, the EU recognized the need for modern means of protection. Therefore, in 1995, the European Data Protection Directive was adopted, establishing minimum standards for data privacy and security, on the basis of which each member state bases its own implementing law [33].

Also the reasons for the said legislation are a number of events, in particular, in 2000, most financial institutions offered online banking. In 2006, Facebook opened to the public [34]. In 2011, a Google user sued the company due to the scanning of his email. Two months after that, the European data protection authority announced that the EU needed a "comprehensive approach to the protection of personal data" and work began on updating the 1995 directive [35]. GDPR came into force in 2016 after being passed by the European Parliament, and as of May 25, 2018, all organizations had to be compliant [33].

In particular, this law stipulates that companies must process customers' personal data in accordance with seven principles:

- legality, fairness and transparency

- purpose limitation. Data must be taken for legitimate purposes clearly stated to the data subject at the time of collection.

- data minimization. The company must collect and process as much data as is necessary for the stated purposes.

- accuracy. Companies must keep personal data accurate and up-to-date.

- retention limits. Companies must retain personal data for as long as necessary for the stated purpose.

- integrity and confidentiality. Data must be processed in a manner that ensures appropriate security, integrity and confidentiality (e.g., through encryption).

- accountability. The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles [31].

In addition, companies or organizations must guarantee the security of user data. In particular, this requires the use of different types of technologies, such as two-factor verification or end-to-end encryption [31].

It should be noted that organizations have a limited ability to accept user data. It should also be added that under the GDPR, users have a number of rights, in particular the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to denial, the right to automated decision-making and profiling.

Another country that is actively fighting cybercrime from a legal perspective is the United States. One example of legislative initiatives in this vein is the Computer Fraud and Abuse Act of 1986 (CFAA) [36]. This is a US cybersecurity bill passed in 1986 as an amendment to an existing computer fraud law that was incorporated into the Comprehensive Crime Control Act of 1984. The law prohibits accessing a computer without authorization or in excess of authorization. Prior

to the enactment of computer-related criminal legislation, computer offences were prosecuted as mail and electronic communication fraud, but the applicable law was often inadequate [37].

Discussion

The original 1984 bill was passed in response to concerns that computer-related crimes might go unpunished [37].

Thus, the CFAA was created to extend existing tort law to intangible property, theoretically limiting federal jurisdiction to cases "that present a compelling federal interest, i.e., where computers of the federal government or certain financial institutions are involved or where the offense itself is interstate in nature," but its broad definitions have tipped into contract law (see "Protected Computer" below). In addition to amending several provisions of the initial Section 1030, the CFAA also criminalized additional computer-related conduct. The provisions address the distribution of malicious code and denial-of-service attacks. Congress also included provisions in the CFAA criminalizing the trafficking of passwords and similar items [37].

Since then, the Act has been amended several times, in 1989, 1994, 1996, in 2001 by the USA PATRIOT Act of 2002, and in 2008 by the Identity Theft Prevention and Recovery Act. With each amendment to the Act, the types of behavior covered by the Act expanded [37].

In the case of China, work in the legal area of cybersecurity has made significant progress. In the last years of the second decade of the 21st century, the government of this country has strengthened the regulation of cybersecurity, data security and the protection of personal information. Thus, since 2016, three important laws have been enacted, namely: The Cybersecurity Law of the People's Republic of China [38]; the Data Security Law of the People's Republic of China [39] and the Personal Information Protection Law of the People's Republic of China [39] have been promulgated to lay the foundation for security regulation in these areas.

The Cybersecurity Law of the People's Republic of China (in Chinese: 中华人民共和国网络安全法) was passed by the National People's Congress to strengthen data protection, data localization, and cybersecurity. in the interest of national security. [38] The law is part of a broader series of laws passed by the Chinese government to strengthen national security legislation. Examples of this since 2014 include the National Intelligence Law, the National Security Law of the People's Republic of China, and laws on counterterrorism and the management of foreign non-governmental organizations. All of these laws were enacted during consecutive intervals [40].

The Cybersecurity Law of the People's Republic of China was passed by the Standing Committee of the National People's Congress on November 7, 2016 and took effect on June 1, 2017. [38] It requires network operators to store selected data in China and allows Chinese authorities to conduct spot checks. on a company's network operations.

As a result of this law, the following aspects have been realized:

- The principle of cyberspace sovereignty established

- Defined the security obligations of Internet product and service providers

- Detailed the security obligations of Internet service providers.

- Further improvement of rules for the protection of personal information

- A security system for key information infrastructure has been established

- Rules for the transnational transfer of data from critical information infrastructures have been introduced.

The Cybersecurity Law applies to network operators and businesses in "critical sectors." [40] By critical sectors, China roughly divides domestic businesses into network businesses engaged in telecommunications, information services, energy transportation, water supply, financial services, government services, and e-government services.

The law applies to all companies in China that operate their own servers or other data networks. Network operators are expected to, among other things, clarify cybersecurity responsibilities within their organization, take technical measures to protect network operations, prevent data leakage and theft, and report any cybersecurity incidents to both network users and the relevant application department for that sector [38].

The Act consists of subsidiary subdivisions of regulations that specify its purpose. For example, its component is the Core Infrastructure Initiative (CII) "Rules for Security Protection and Security Assessment Measures for Cross-Border Transmission of Personal Information and Sensitive Data" [41]. [41]. However, this law needs to be further refined as Chinese government authorities are busy identifying more laws that are better suited to the cybersecurity law. Thus, by incorporating existing VPN laws and data security into the cybersecurity law, the Chinese government is strengthening its oversight as well as emphasizing the need for foreign companies to comply with national regulations. [40]

The Data Security Law of the People's Republic of China was enacted in 2016 to regulate the collection, storage, use, transfer and processing of data in China [39]. According to this law, all organizations and citizens in China are required to protect data security and ensure that the confidentiality of personal data is adequately protected. The law also requires organizations that collect and process data to implement the necessary technical and organizational measures to ensure data security. Organizations must also report any data leakage or data security breach.

The Personal Data Protection Law of the People's Republic of China was enacted in 2018 to regulate the collection, use, and transfer of personal data [42]. The law establishes rules for the collection of personal data, such as users' consent to the collection and use of their data. According to this law, organizations must ensure adequate security of personal data and not collect more data than necessary to perform their functions. Organizations must also notify users about how their personal data will be used and provide access to their personal data upon request. By analyzing these laws, it can be concluded that China is making efforts to ensure data security and privacy of personal data of its citizens and organizations. These laws establish rules and requirements for the collection, storage, transfer, and use of data, and require organizations to implement necessary data security measures.

The Personal Data Protection Act also establishes rules for the collection of personal data and requires organizations to inform users about how their data will be used and to provide access to their personal data upon request. This allows users to control the use of their personal data and protect their privacy [42].

In general, China's data protection laws are aimed at ensuring data security and protecting users' rights, as well as improving data management in the country. However, it should be noted that

some aspects of these laws may be challenged or further addressed over time, as data protection law is a constantly evolving area.

By comparing the legislative systems discussed above, it can be concluded that they reflect the worldview and political characteristics of each country. In particular, the cyberlaws of the European Union are based on fundamental declarations upholding human rights and freedoms. This is also characteristic of the United States, but it is worth noting that this country is a state dominated by a system of common law or case law, which is reflected in the law discussed above. In turn, China's worldview is different from the “Western” one, and the dominant ideas in this country are pragmatic and authoritarian. Thus, cyber law in China emphasizes data control rather than the protection of users' rights.

Conclusion

As for the Central Asian countries, the issue of cybersecurity legislation is at a rather low level. In particular, only Kazakhstan has the Law “On Information, Informatization and Information Protection,” which was adopted in 2013 to ensure the protection of information in electronic form from illegal access, use and dissemination [43]. The law regulates the protection of personal data, prohibits illegal access to information, establishes liability for violation of information protection rules, including criminal liability for cybercrime. The law also provides for the establishment of a national information protection system, including the creation of a national computer coordination center.

Despite the fact that there is such a law, in general, this sphere is not very developed, so an important aspect is the borrowing and introduction of experience of foreign countries in the countries of Central Asia.

Thus, one possible form of assistance to China in the area of cyber law could be to organize seminars and trainings for representatives of Central Asian countries on cyber security and cyber defense. China can offer its experts who can provide training and advice on cyber security, cyber defense, cyber attacks and other important aspects.

In addition, China can provide material assistance to Central Asian countries in developing and implementing cybersecurity laws. For example, it can provide technical support, software, equipment and other resources that can help countries with cybersecurity.

China can promote cyber security through its Silk Belt and Sea Route project, which covers most Central Asian countries. This project can be a platform for cooperation between China and Central Asian countries on cybersecurity.

Overall, China's assistance in establishing cybersecurity laws in Central Asian countries can make an important contribution to the development of cybersecurity in the region and provide better protection against cyberattacks and other cyber threats.

It is also important to note that China already has experience in cooperating with Central Asian countries in this area. For example, within the framework of the Shanghai Cooperation Organization (SCO), a joint working group on cyber security was established, called the Working Group on Information Security. 44] The group was established in 2002 at a meeting of SCO foreign ministers.

The purpose of the group was to ensure that SCO countries cooperate in cybersecurity and coordinate efforts to combat cybercrime. 44] The working group discusses cybersecurity and cyber defense, cyber infrastructure development, and other issues.

The working group includes consultations and discussions on developing and improving national cybersecurity strategies, establishing cyber defense standards and protocols, developing joint action plans to address cybersecurity issues, sharing cyber defense expertise, and more.

Thus, continued cooperation within the SCO framework could become an essential element in the development of cyber security in Central Asian countries. In general, cooperation with China is quite promising for the countries of the region. Since China has considerable experience in cyber security, its development in Central Asia is beneficial for both China and the countries of the region.

References

Mattord H. Principles of Information Security. – Boston: Cengage Learning. 2023. – 471 p.

Shuai C. Exploring the global geography of cybercrime and its driving forces // Humanities and Social Sciences Communications. – 2023. V. 10, №1. – P. 839-851.

Haralambos M. Modelling language for cyber security incident handling for critical infrastructures // Computers and Security. – 2023. V. 128, №1. – P. 23-38.

Jakub D. Drop Weight Testing of Samples Made of Different Building Materials Designed for the Protection of Classified Information // Materials. – 2023. V. 16, №3. – P. 501-513.

Ilina D. Analytical model of actions of the information security violator on covert extraction of confidential information processed on the protected object // Wave Electronics and its Application in Information and Telecommunication Systems, WECONF 2021 - Conference Proceedings. – 2021. V. 3, №5. – P. 381-394.

Mohan P. Secure Database Authentication from Vulnerability Detection using Encryption Mode of Standardization // 8th International Conference on Smart Structures and Systems. – 2022. V. 6, №3. – P. 207-218.

Krutskikh A. International Information Security: In Search of Consolidated Approaches // Vestnik RUDN. International Relations. – 2022. V.22, №2. – P. 341-352.

Power R. Secrets Stolen, Fortunes Lost: Preventing Intellectual Property Theft and Economic Espionage in the 21st Century. – Krakow: Syngress. 2011. – 278 p.

The latest government data breaches in 2020/2021. 2021. https://portswigger.net/daily-swig/the-latest-government-data-breaches

Nearly 7 lakh cyber attacks in 2020, IT Ministry tells Parliament. 2020. https://www.hindustantimes.com/india-news/nearly-7-lakh-cyber-attacks-in-2020-it-ministry-tells-parliament/story-bOv6SuWSP9XxUwtF9uBTvK.html

Cyberattack on German Government. 2018. https://www.synergiafoundation.org/insights/analyses-assessments/cyberattack-german-government

Must-Know Ransomware Statistics. 2022. https://www.antivirusguide.com/cybersecurity/ransomware-statistics/?gclid=Cj0KCQiA9YugBhCZARIsAACXxeJAi0RRs96et0m8PjFcKQy9ur3ZqPK1kWRGSL65X3OiqwVwL51FUHcaAt7JEALw_wcB

Man Q. Fighting cybercrime: Legislation in China // International Journal of Electronic Security and Digital Forensics. – 2008. V. 2, №2. – P. 219-227.

Ying-Yu L. China cyber warfare and cyber force // Tamkang Journal of International Affairs. – 2019. V. 22, №3. – P. 119-162.

China's Ministry of Industry and Information Technology (MIIT).

http://english.www.gov.cn/state_council/2014/08/23/content_281474983035940.htm
Report on the Work of the Government. 2009. http://www.npc.gov.cn/zgrdw/englishnpc/Special_11_5/2010-03/03/content_1690628.htm\
Hong Kong exchange hit by hackers. 2011. https://www.ft.com/content/f448a9b6-c33a-11e0-9109-00144feabdc0
Toy firm VTech hack exposes private data of parents and children. 2015. https://www.theguardian.com/technology/2015/nov/30/vtech-toys-hack-private-data-parents-children
What is WannaCry ransomware and why is it attacking global computers? 2017. https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20
$1.1 billion in cryptocurrency has been stolen this year, and it was apparently easy to do. 2018. https://www.cnbc.com/2018/06/07/1-point-1b-in-cryptocurrency-was-stolen-this-year-and-it-was-easy-to-do.html
Chinese cyberattackers compromising telcos in Southeast Asia for espionage. 2019. https://www.csoonline.com/article/3628719/chinese-cyberattackers-compromising-telcos-in-southeast-asia-for-espionage.html
Ismailova R. Cybercrime risk awareness rate among students in Central Asia: A comparative study in Kyrgyzstan and Kazakhstan // Information Security Journal A Global Perspective. – 2019. V. 28, №1. – P. 141-162.
Кибератаки: преступление и наказание. 2015. https://www.currenttime.tv/a/26981442.html
Биткоины в "фонд ФСБ": как исчезли $450 млн с криптобиржи Wex. 2019. https://www.bbc.com/russian/features-50420738
Cobalt in Kazakhstan. 2020. https://oec.world/en/profile/bilateral-product/cobalt/reporter/kaz
Cobalt: Their Evolution And Joint Operations. 2021. https://www.group-ib.com/resources/research-hub/cobalt-evolution/
The NIS Directive. 2016. https://www.nis-2-directive.com/
ENISA. https://www.enisa.europa.eu/
GDPR. https://gdpr-info.eu/
European Convention on Human Rights. https://www.echr.coe.int/documents/convention_eng.pdf
Bekkum M. Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception? // Computer Law and Security Review. – 2023. V. 48, №1. – P. 739-756.
Facebook Expansion Enables More People to Connect with Friends in a Trusted Environment. https://about.fb.com/news/2006/09/facebook-expansion-enables-more-people-to-connect-with-friends-in-a-trusted-environment/
US woman sues Google over Gmail scanning. https://www.computerweekly.com/news/2240105327/US-woman-sues-Google-over-Gmail-scanning
Text of the Computer Fraud and Abuse Act. https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781119231899.app4
Johnson L. Governmental Laws, Policies, and Procedures // Computer Incident Response and Forensics Team Management. – 2014. V. 4, №2. – P. 481-503.
中华人民共和国网络安全法 [现行有效] . http://www.lawinfochina.com/Display.aspx?LookType=3&Lib=law&Id=22826&SearchKeyword=&SearchCKeyword=&paycode=
中华人民共和国数据安全法 . http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml
中华人民共和国个人信息保护法 .

http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml
Lai Y. Securitisation or Autocratisation? Hong Kong's Rule of Law under the Shadow of China's Authoritarian Governance // Journal of Asian and African Studies. – 2023. V. 58, №1. – P. 8-25.
Закон «Об информации, информатизации и защите информации». https://studwood.net/1509929/pravo/zakon_informatsii_informatizatsii_zaschite_informatsii
SCO Expert Group on International Information Security. http://eng.sectsco.org/news/20191112/600393.html
How Can Foreign Technology Investors Benefit from China's New Infrastructure Plan? https://www.china-briefing.com/news/how-foreign-technology-investors-benefit-from-chinas-new-infrastructure-plan/
Passenger name record data. https://www.gov.uk/government/publications/passenger-name-record-data/passenger-name-record-data
Terrorist Financing Tracking Program. https://home.treasury.gov/policy-issues/terrorism-and-illicit-finance/terrorist-finance-tracking-program-tftp.