The Current Situation and Legal Countermeasures to Cybercrimes in the Republic of Uzbekistan

Bobirjon Izzatullaev, Leading Specialist
Research Institute of Legal Policy

INTRODUCTION

With the growing penetration of digital technologies, cyber security has become an essential part of national security. According to the recommendations of UN experts, the term "cybercrime" covers any crime that can be committed using a computer system or network.[1]

The U.S. Department of Justice divides cybercrime into three categories:[2]

1. crimes in which the computing device is the target - for example, to gain network access;
2. crimes in which the computer is used as a weapon - for example, to launch a denial-of-service attack; and
3. crimes in which the computer is used as an accessory to a crime - for example, using a computer to store illegally obtained data.

The Council of Europe Convention on Cybercrime, to which the U.S. is a signatory, defines cybercrime as a wide range of malicious activities, including the illegal interception of data, system interferences that compromise network integrity and availability, and copyright infringements.[3]

Cybercrimes were already increasing before the pandemic, but since 2019, cybercrime statistics show that the whole world was impacted by COVID-19. Cybercrime up 600% Due to COVID-19 Pandemic and cost makes up a value worth 1% of the Global GDP.[4]

This upward trend in cybercrime is also observed in Uzbekistan. The Ministry of Internal Affairs of the Republic reports that cybercrime has increased by 8.3 times over the past 3 years in Uzbekistan. Therefore, in recent years, Uzbekistan

---

[1] Киберпреступность: история развития, проблемы практики расследования. // Анна Борисовна Николаева, Марина Владимировна Тумбинская // https://www.computer-museum.ru/articles/materialy-mezhdunarodnoy-konferentsii-sorucom-2014/629/

[2] Kate Brush, Linda Rosencrance, Michael Cobb – Cybercrime. https://www.techtarget.com/searchsecurity/definition/cybercrime

[3] Kate Brush, Linda Rosencrance, Michael Cobb – Cybercrime. https://www.techtarget.com/searchsecurity/definition/cybercrime

[4] The Cost of Cybercrime. https://purplesec.us/resources/cyber-security-statistics/

has been actively developing new special laws against cybercrime, amended their national legislation or codes, adding specific paragraphs to address cybercrime.

This opinion article reviews growing trends of cybercrime in Uzbekistan, its current status and legal measures to combat in the country.

THE GROWING TREND OF CYBERCRIME IN THE WORLD AND UZBEKISTAN

Any information and technical innovations significantly expand the scope of cybercrime and create conditions for increasing the effectiveness of hacker attacks. Therefore, cybercrime is growing at a faster rate than all other types of crime. According to cybercrime magazine, cybercrimes cost more than $6 Trillion in 2021.[5]

Cybersecurity Ventures expects global cybercrime costs to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015.[6]

Kaspersky has released a new report revealing a growing number of cyber-attacks on small businesses in 2022 so far. Researchers compared the period between January and April 2022 to the same period in 2021, finding increases in the numbers of Trojan-PSW detections, internet attacks and attacks on Remote Desktop Protocol.[7]

According to the statistics, globally, 30,000 websites are hacked daily, 64% of companies worldwide have experienced at least one form of a cyber-attack, Email is responsible for around 94% of all malware, every 39 seconds, and there is a new attack somewhere on the web.[8]

A record growth rate in the number of network users in Uzbekistan has been observed in the past ten years. According to the Ministry for Development of Information Technologies and Communications of the Republic of Uzbekistan, the number of Internet users is more than 27.2 million people.[9]

Over the five months of 2021 year, more than 330 crimes were committed in Uzbekistan using computer technology in the financial, credit and banking and other areas.[10] During the monitoring of the national segment of the Internet, 342

[5] The Cybercrime 2022 Watchlist. https://right-hand.ai/blog/the-cybercrime-2022-watchlist/
[6] Cybercrime To Cost The World $10.5 Trillion Annually By 2025. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
[7] Report: Frequency of cyberattacks in 2022 has increased by almost 3M. https://venturebeat.com/security/report-frequency-of-cyberattacks-in-2022-has-increased-by-almost-3m/
[8] How Many Cyber Attacks Happen Per Day in 2022? https://techjury.net/blog/how-many-cyber-attacks-per-day/#gref
[9] The number of Internet users in Uzbekistan exceeds 27.2 million people. https://www.uzdaily.com/en/post/70654
[10] Сообща противостоять киберпреступности. https://xs.uz/ru/post/soobscha-protivostoyat-kiberprestupnosti

information security incidents were recorded in relation to the websites of the "UZ" domain zone.[11]

Currently, there are often cases of theft of funds from bank debit/credit cards of citizens. To date, more than 600 crimes committed with the use of information technology have been identified in this sphere.[12] In 2020, the Cybersecurity Center received data on more than 27,000,000 events of malicious and suspicious activity through various channels.[13]

In the Republic of Uzbekistan, the following types of crimes represent cybercrimes:

- Crimes in the field of information technology;
- Elements of traditional crimes committed using ICT (for example, inducing suicide using telecommunications networks, theft with unauthorized entry into a computer system);
- Elements of crimes related to information security (for example, distribution of materials containing a threat to public safety and public order, dissemination of false information in telecommunications networks).

The majority of virtual crimes in Uzbekistan occur with the use of modern information and communication technologies. There is the theft of funds from bank debit/credit cards, the distribution and illegal sale of narcotic and psychotropic substances, fraud, and extortion.

THE LEGAL RESPONSE TO CYBERCRIME IN UZBEKISTAN

Ensuring cybersecurity is regulated by by-laws, such as the Decree of the President of the Republic of Uzbekistan "On measures to implement the state system for protecting information systems and resources of the Republic of Uzbekistan" (adopted November 21, 2018), "On additional measures to improve the system of control over the introduction of information technologies and communications, the organization of their protection" (September 14, 2019) and "On measures to further improve the cybersecurity system in the Republic of Uzbekistan" (adopted June 15, 2020).

---

[11] Кибербезопасность – проблема общая. О Международном экспертном форуме СНГ. https://e-cis.info/news/566/95743/

[12] Как бороться с киберпреступностью? https://strategy.uz/index.php?news=1150&lang=ru

[13] Киберпреступность стала глобальной проблемой и требует глобального противодействия. https://yuz.uz/ru/news/kiberprestupnost-stala-globalnoy-problemoy-i-trebuet-globalnogo-protivodeystviya

In addition, the laws "On Telecommunications", "On Informatization", "On Personal Data" regulate the activities of bodies responsible for the implementation of state policy in the field of information security.

The Law of the Republic of Uzbekistan “On Cybersecurity” (adopted March 15, 2022) is directly aimed at regulating public relations in the field of cybersecurity. The law consists of 8 chapters, includes 40 articles. The Law is aimed at regulating relations in the field of ensuring cybersecurity in the cyberspace of the Republic of Uzbekistan.

The law (“On Cybersecurity” adopted March 15, 2022) reveals the basic concepts that were not previously clearly defined by law. The law defines the concept of critical information infrastructure objects, which is actually very important. The following positive aspects of the Law are clearly articulated principles.

In general, it can be said that law and acts on cybersecurity include that they establish requirements for ensuring the cybersecurity of information systems and resources of state bodies and organizations, responding to cyber-attacks and ensuring the effective operation of the main bodies regulating cybercrime in Uzbekistan. In addition, an effective legal framework is being created for the promotion and further development of the domestic cybersecurity industry, the adoption of state support measures, and the training of cybersecurity specialists. Moreover, this contributes to the creation of an effective legal framework for the further development of the domestic sphere of cybersecurity, the adoption of state support measures and the training of cybersecurity specialists.

There are following agencies in charge of regulatory cybercrimes in Uzbekistan.

Firstly, the State Security Service of the Republic of Uzbekistan is an authorized state body in the field of cybersecurity.

Secondly, the State Inspectorate for Control in the Field of Informatization and Telecommunications of the Republic of Uzbekistan control over compliance with legislative acts in the field of communications, informatization and telecommunication technologies.

Thirdly, the State Unitary Enterprise “Cybersecurity Center” is a single state institution providing analysis of information on computer incidents, advisory and technical support in preventing computer security threats in Uzbekistan.

It is important to note that in 2020, by the Decree of the President, the Strategy "Digital Uzbekistan - 2030" was approved and is being consistently implemented in the republic. In the coming years, it is planned to implement more

than 1,620 projects for the digital transformation of regions and industries.[14] The strategy also provides for the solution of a wide range of long-term issues related to the introduction of digital technologies in the field of telecommunications, public services, the real sector of the economy, healthcare, the state inventory, etc.

The main principles of ensuring cybersecurity are: legality; the priority of protecting the interests of the individual, society and the state in cyberspace; a unified approach to regulating the sphere of cybersecurity; priority for the participation of domestic manufacturers in the creation of a cybersecurity system; openness of the Republic of Uzbekistan to international cooperation in ensuring cybersecurity. The unified state policy in the field of cybersecurity is determined by the President of the Republic of Uzbekistan.

REGIONAL COOPERATION OF UZBEKISTAN IN CYBER SECURITY

Both national legislation and international law are directly relevant to cybersecurity. In the Commonwealth of Independent States (CIS), in the field of ensuring information security, the "Agreement on information interaction of the CIS member states in the field of digital development of society", "Strategy for ensuring information security of the CIS member states", "Agreement on cooperation of the CIS member states in the field of information security" were adopted.

On June 29, 2021, Tashkent hosted the CIS International Expert Forum on Information Security, which was held at the initiative of the President of Uzbekistan.[15] In addition, particular attention is paid to cooperation in the field of cybersecurity within the framework of the Shanghai Cooperation Organisation (SCO).

THE IMPORTANCE OF LEGAL COUNTERMEASURES TO CYBERCRIMES

The legislation plays an important role in combating cyber threats. The legal framework includes the creation of legislation that establishes the concept of illegal activities in cyberspace, together with the definition of the necessary procedural tools for investigating and enforcing such legislation. Legislation is a dynamic tool that allows the state to respond to new social and security issues. It provides a

[14] Digital Uzbekistan 2030 Strategy envisages several breakthrough measures for the country's development/ http://isrs.uz/en/smti-ekspertlari-sharhlari/eldor-aripov-strategia-cifrovoj-uzbekistan-2030-predpolagaet-rad-proryvnyh-dla-strany-mer

[15] Tashkent hosts CIS International Expert Forum on Information Security. https://uzbekembassy.com.my/eng/news_press/politics/tashkent_hosts_cis_international_expert_forum_on_information_security.html

balance between the protection of privacy and the fight against crime, establishes the responsibility of subjects of legal relations in the field of cybersecurity.

As computers and the internet take over the world and every part of our lives, cyber laws are becoming increasingly important. Cyber laws regulate the digital exchange of information, e-commerce, software, information technology, and monetary activities. Cyber law encompasses all of these legal structures and regulating mechanisms, and these laws are critical to the success of electronic commerce.[16]

Just like any other law, cyber law consists of rules that dictate how people and companies should use the internet and computers. While other rules protect people from getting trapped in cybercrime run by malicious people on the internet. Although it is close to impossible to curb 100% of all cybercrimes. The importance of cyber law can be understood by the following points:

- it dictates all actions and reactions in Cyberspace;
- all online transactions are ensured to be safe and protected;
- all online activities are under watch by the Cyber law officials;
- security for all data and property of individuals, organizations, and Government;
- helps curb illegal cyber activities with due diligence;
- all actions and reactions implemented on any cyberspace has some legal angle associated with it;
- keeps track of all electronic records;
- Helps to establish electronic governance.

CONCLUSION

Along with the widespread use of information technology in the world, there is an increase in the number of crimes in this area. Cybercrime is characterized by a high level of economic damage.

In recent years, large-scale work has been carried out in the Republic of Uzbekistan to develop legal measures, modernize state programs, and ensure information security to combat cybercrime. Creating an effective regulatory framework will have a preventive effect on cyber threats, and therefore ensuring national cyber security directly depends on the availability of effective legal mechanisms.

To implement an effective policy to cybercrime, the following measures should be taken:

[16] The role of cyber law in cyber security in India by Sankalp Mirani. https://legalresearchandanalysis.com/current-affairs/the-role-of-cyber-law-in-cyber-security-in-india

- training of qualified specialists in this field;
- the widest possible use of block chain technology to counter cyber threats;
- development of artificial intelligence resources and their consistent implementation in the field of cybercrime investigation;
- tougher laws to fight cybercrime.

Moreover, ensuring security in the information sphere requires extraordinary collective approaches. It is practically impossible to control cybercrime and fight it at the level of an individual state. The adoption of international norms and standards should be accompanied by changes in the national legislation of states. Coordination of the efforts of states is necessary to ensure a rapid response to the development of computer technology and the adoption of appropriate regulations.