International Journal of Cyber Law | Volume: 1 Issue: 3 2023

# Comparative Analysis of the USA and Uzbekistan in Ensuring Cyber Security

**Hamroyev Ulug'bek Rustamovich**
Customs Institute of Customs Committee
uzbekiston@inbox.ru

**Rahmatullayeva Bahora Mirjaxon qizi**
The Cadet of Customs Institute
rahmatullaevabahora6@gmail.com

## Abstract

This thesis describes the measures and measures taken by the US state to combat cybercrime, which is one of the most urgent issues today, and their negative and positive consequences. At the same time, information security between Uzbekistan and the US The analysis of the work being carried out in order to ensure it is presented in the form of a table. In addition, the work that should be carried out in order to prevent various cyber-attacks is given as a proposal.

**Keywords:** Cybercrime, Phishing Attacks, Confidentiality, Authentication, Identification, FISMA, UZ-CERT Service.

## I. Introduction

Cybercrime is a criminal activity aimed at abusing a computer, computer network, or a networking device. Many of them are committed by cybercriminals or hackers with the aim of earning an illicit gain from it. While cybercrime is a relatively new concept, it has a negative impact on the economy of many countries. Polls show that more than 500 million cyberattaks are launched worldwide every year. Every second, one in 12 people become victims of cyberspace attacks. In developed countries such as the United States, France, England, Germany, Belgium, and Luxembourg, 60-65 percent of crimes are committed through cyber attacks. In the last three years , crimes of this type have also increased by 8.3 times

in the country, reaching about 5 percent of the total crime now [1]. Internet users suffer enormous economic losses as a result of not knowing how to protect against these cyberattacks, which are a major threat to us.

## II. Methodology

In this study, a comparative analysis of the USA and Uzbekistan in ensuring cyber security will be conducted using a mixed-method research design. The study will utilize both quantitative and qualitative methods to gather data and analyze the findings. The quantitative data will be collected through a survey questionnaire distributed to a sample of cyber security professionals and experts from both countries. The qualitative data will be obtained through in-depth interviews with key informants such as government officials, cyber security analysts, and academics. The data collected will be analyzed using descriptive statistics and thematic analysis to identify patterns, similarities, and differences between the two countries in ensuring cyber security. To establish a methodological connection, this study will draw on theories and concepts related to cyber security, such as the Cybersecurity Framework developed by the National Institute of Standards and Technology (NIST) and the Five Pillars of Cybersecurity by the World Economic Forum (WEF). Additionally, the study will also utilize comparative analysis, which is a research methodology that involves comparing two or more entities, in this case, the USA and Uzbekistan, to identify similarities and differences in their approach to cyber security.

Data collection will be conducted through both primary and secondary sources. The primary data will be collected through the survey questionnaire and in-depth interviews with key informants, while the secondary data will be collected through a review of relevant literature, reports, and publications on cyber security issues in the USA and Uzbekistan. The survey questionnaire will be administered online using a snowball sampling technique, and the in-depth interviews will be conducted face-to-face or virtually with the key informants. The data collected will be recorded, transcribed, and analyzed using appropriate software. One potential

limitation of this study is the availability and reliability of data in Uzbekistan, given the country's limited transparency and openness. Additionally, the study's scope is limited to a comparative analysis of two countries, and the findings may not be generalizable to other countries or regions. Finally, the study's reliance on self-reported data from the survey questionnaire may introduce bias and inaccuracies in the findings. To mitigate these limitations, the study will utilize multiple sources of data and triangulation of findings to enhance the validity and reliability of the results.

## III. Results

Through the following comparative Table 1, we will have an overview of the occurrence of cybercrime in the United States and the country:

**Table 1**

| S/R | *USA* | *Uzbekistan* |
|---|---|---|
| **1** | **The emergence of cyberbullying** | |
| | On November 2, 1988, a computer-to-computer smart program appeared on the Internet at the Massachusetts Institute of Technology (MIT) in the United States.This was the first manifestation of cyberbullying. | Since the 2010s, cybercrimes and cyberthreats have begun to increase in the country |
| **2** | **The most common types of cyberbullying** | |
| | • Malware Based Attacks (ransomare,Trojans,etc.)<br>• Middle Human Attack (MITM)<br>• Phishing attacks<br>• Financial risk the theft of bank card payment information;<br>• Identity fraud (when personal data is stolen and used). | Fraudsters seize the codes in the SMS notification that came to plastic card users through excuses such as making payments, giving them success, and absorbing the funds in it<br>fraud by acquiring and disclosing personal information<br>• intimidation, insults, suicidal situations (cyberbulling) and so on with the use of violence on social media. |
| **3** | **The rate at which a cyberbullying occurs** | |

| | | |
|---|---|---|
| | According to the Security Journal, there are more than 2200 attacks every day, which corresponds to 39 cyberbullying every 1 second. [7] | On average, more than 17 million cases of malicious and suspected network activity are diagnosed each year. There have been more than 1,3 million cyberspies on websites. |
| **4** | **Government agencies fighting cybercrime** | |
| | 1)Federal Bureue of Investigation FBI<br>2) Department of Homeland Security (DHS) | 1) Department of Combating Cybercrime of the Ministry of Internal Affairs of the Republic of Uzbekistan<br>2) Cybersecurity Center<br>3) Ministry of Internal Affairs |
| **5** | **Basic Laws Relating to Cybersecurity** | |
| | 1) Health Insurance Portability and Accountability Act **(HIPAA)**<br>2) **Gramm-Lich-Bliley** qonuni<br>3) National Security Act **(FISMA)** | 1) Law of the Republic of Uzbekistan No. NQ-764 of 15.04.2022<br>2) "Information Technology Act" (11.12.2003)<br>3) Law of the President of the Republic of Uzbekistan "On additional measures for the protection of national information resources" (8.08.2011) |
| **6** | **Work in place to prevent and stop cybercrime:** | |
| | The government has launched a National Cybercrime Reporting Portal *(www.cybercrime.gov.in)* to allow the public to report incidents involving all types of cybercrime, with a special focus on cybercrime against women and children. | Several organizations have been set up to ensure cybersecurity:<br>https:// my.gov. Uz/uz/ -Single portal of interactive government services<br>Www. Unicon. Uz – Center for Science and Marketing Research<br>3. Uz-CERT service set up against hackers on the Internet |
| **7** | **Types of penalties used for cybercrime** | |
| | Theft of computer-related personal information, which includes unauthorized acquisition, use or misuse, possession and transfer, modification or deletion of identity information of another person, is punishable by up to six months in prison and hundreds of thousands in fines<br>• Life in prison for computer system infringing | A number of provisions of the Criminal Code provide for crimes committed using computer technology and liability against them.<br>For example, Article 278 of this Code states intentionally firing someone else's computer device, as well as disrupting the computer system (computer sabotage):<br>Deprivation of certain rights for up to three years and fines ranging from 66 million 900,000 hours to 89 million 200,000 hours;<br>2 yilgacha ozodlikni cheklash;<br>Punishable by imprisonment for up to 2 |

| | | |
|---|---|---|
| | | years.<br>Also, committing these acts as a group, repeatedly or by a dangerous retsidivist, can result in imprisonment of up to three years. |

## IV. Discussion

Cybersecurity is a strategic issue for each country. In many ways, U.S. activism in cybersecurity issues in the world is higher than in other countries. There are 1.5 million cyberbullying incidents in Washington every year, or more than 4,000 attacks per day, 170 attacks every hour, or almost three attacks every minute. In 2019 an estimated $1.5 billion was lost in the United States as a result of fraud on online credit and debit cards **[2].** In a 2020 Global Risk Report, the World Economic Forum reported that the likelihood of identifying and prosecuting cybercriminals in the United States is less than 1 percent.In the UNITED States, the FBI and the Department of Homeland Security (DHS) are government agencies that fight cybercrime. The FBI has deployed trained cybercrime-trained agents and analysts in its offices and headquarters. According to DHS, the Secret Service has a cyber intelligence unit that works to target financial cyber crimes. They use their intelligence information to protect against international cybercrime. Their efforts are aimed at protecting institutions such as banks from aggression and information breaches.

### A. The most common types of cybercrime in the United States:

i. Fraud in e-mail and the Internet;
ii. Identity fraud (when personal data is stolen and used);
iii. Financial risk i.e. the theft of bank card payment information;
iv. theft and sale of corporate data;

v. Cyber fraud (requesting money to prevent a threatened attack);
vi. Ransomware hujumlari (grew tovlamachilikning well shows) [3].

According to statistics, an estimated 53.35 million US forces were affected by cybercrime in the first half of 2022, and between July 2020 and June 2021, the United States was the most targeted country for cyberbullying, accounting for 46 percent of global attacks. US citizens lost $ 2021 billion due to cyber crimes, including computer fraud ($ 956 million), investment fraud ($ 1,4 billion), and business email ($2,39 billion). The cost of eliminating these attacks in 2021 will average $1,08 million, down 49% from 2020 ($2,09 million) [4]. Only 50% of US organizations have fully insured cyber insurance. Most alarmingly, it is that 1 in every 10 US organizations (12%) are not protected from cyberbullying and could be financially devastated if they are attacked. In an attempt to curb, curb cybercrime, the United States developed its own cybersecurity strategy by the early 2000s.

**B. In its cybersecurity strategy, the US focuses primarily on the following objectives:**

i. Achieving the co-operation of public and private sectors to protect important infrastructures.
ii. Developing plans for developing the ability of the public and private sectors to act together, encouraging the private sector to carry out tasks in the cyber sphere and supporting it along the way.
iii. Increase the 'immunity' of employers and the business sector against cyberbullying, focusing on educating and directing at the federal level.
iv. Formulate plans to eliminate threats that arise in the wake of Russia's cyber power.
v. Constant introduction of technological innovations into practice in order to prevent China's threats of cyber-espionage and take the

necessary measures to protect the commercial interests of the private sector.

vi. Protection of all official computers, software and networking technologies in agriculture, food, drinking water, public health and emergency response systems, social security, information and telecommunications infrastructure, energy, transportation, banking and finance, chemistry, postal systems from cyberbullying.

vii. Ensuring the free movement of goods and services, ideas, entrepreneurs and capital.

viii. Support these countries in the fight against cybersquassions aimed at destabilizing countries allied with the United States [5].

In the first half of 2020, the number of fraud offenses in the country also doubled compared to a year ago, reaching 3,881 in six months. Moreover, as technology progresses, new types of fraud are emerging [6]. The most common of them are with bank plastic cards. Payment through them has been recognized as the most convenient method and is widely used in practice. The fact that no one can use a plastic card even if it disappears is a guarantee of funding protection. To assist individuals desiring to benefit the worldwide work of Jehovah's Witnesses through some form of charitable giving, a brochure entitled Charitable Planning to Benefit Kingdom Service Worldwide has been prepared. We know that the Internet limits the ability to obtain information through suspicious sources, download informal applications, and respond to ads and e-mails. Today, we usually protect our information by using identification (digital, graphical code, password), authentication, and authorization methods. However, it is also intended to use authentication methods to strengthen information security and maintain them using reliable methods. Especially by using a one-time password or biometric methods, we will be able to maximize protection of information and personal data. For example, the following forms of biometric methods are now common:

1. **Facial recognition (**this biometric authentication method involves measuring certain parameters of human facial structure, for example: eye, eyebrow nose, precisely remember how the mouth is located, size, structure);
2. **Fingerprint scanning** (the uniqueness of each fingerprint allows you to use this biometric authentication method both in forensics and in the process of serious business operations and in everyday life);
3. **Scan retinal** (Retinal scans are much larger and costlier than fingerprint scanners. However, the reliability of this type of authentication is much higher than that of fingerprints. The features of drawing the blood vessels of the fundus are that it is not repeated even in twins. Therefore, such authentication has maximum protection);
4. **Voice recognition** (will clearly remember your voice and open only to the same sound. Defeat is one of the most reliable methods of protection.
5. **Hand geometry authentication** - this biometric authentication method involves measuring certain parameters of the human hand. Examples: the length, thickness and curvature of the fingers, the general structure of the hand, the distance between the joints, the width and thickness of the hand.

## Conclusion

Instead, it should be noted that cybersecurity is one of the most pressing problems of the 21st century. Information does not choose a boundary; it does not recognize virtual barriers. In order to combat these cyberbullying, new approaches to combating cybercrime are being implemented in states. We learned that the United States, considered a developed country in all aspects of the foregoing today, has developed and implemented a strategy to combat cybercrime. As a result of the foregoing, we propose the following proposals to improve the efficiency of measures aimed at ensuring cybersecurity, prevent violations committed over the Internet, and strengthen the legal foundations of the industry:

- Use of licensed and certified operating systems and applications;
- Use security plugins with malware search, deletion and protection functions;
- Install antivirus software in the media and use strong passwords;
- Post personal information only on secure sites;
- Use of modern authentication methods to protect personal and confidential information (Retina scan, hand geometry authentication);
- Apply to any business and financial structures not by e-mail, but through the contacts indicated on the official website;
- It is necessary to establish a restriction on certain sites by the government and to investigate sites that hinder the development of society (in India's case, they have blocked the TIK TOK application);
- To assist individuals desiring to benefit the worldwide work of Jehovah's Witnesses through some form of charitable giving, a brochure entitled Charitable Planning to Benefit Kingdom Service Worldwide has been prepared.

## References:

1. 1.https://iiv.uz/news/
2. https://www.spot.uz/oz/2021/07/16/cyber-usa/
3. https://www.bluevoyant.com/
4. https://aag-it.com/the-latest-cyber-crime-statistics
5. https://kun.uz/uz/28352354
6. https://kun.uz/uz/news/2020
7. https://www.amerikaovozi.com/a/a-36
8. Salayev N.S., Ro‘ziyev R.N. Kiberjinoyatchilikka qarshi kurashishga oid milliy va xalqaro standartlar. Monografiya., – T.: TDYu, 2018, 139-b.
9. Karpova D.N. Kiberprestupnost: globalnaya problema i yeyo reshenie. //Vlast. №8. 2014. S. 46-50.