International Conference of
Economics, Finance and Accounting Studies

International Conference of Economics, Finance and Accounting Studies is a double-blind peer-reviewed, open-access journal published to reach excellence on the scope. It considers scholarly, research-based articles on all aspects of economics, finance and accounting. As an international congress aimed at facilitating the global exchange of education theory, contributions from different educational systems and cultures are encouraged. It aims to provide a forum for all researchers, educators, educational policy-makers and planners to exchange invaluable ideas and resources.

Modern Methods of Combating Cybercrime in the Republic of Uzbekistan

Qo‘ldoshev Sherzod Shukurullo o‘g‘li
Teacher at Tashkent State University Law

Introduction.

Like many other countries, Uzbekistan has a difficult time fighting cybercrime. It uses a combination of international collaboration, technology advancements, and regulatory frameworks to address this changing threat. However, for strategic and security considerations, specifics about certain modern techniques are frequently not made public. However, based on broad patterns and the facts at hand, we can deduce a few plausible strategies:

Regulatory and Legal Frameworks:

Laws pertaining to cybersecurity: To control cyberspace and combat cybercrime, Uzbekistan has passed a number of laws and decrees. These most likely address topics like electronic transactions, data protection, and the investigation and prosecution of cybercrimes. Nonetheless, enforcement is crucial to these regulations' efficacy.

Strengthening digital identity and authentication: To stop fraud and identity theft, better digital identity verification and authentication systems are essential. In order to safeguard online transactions and services, Uzbekistan is probably investing in these areas.

International collaboration: Working together with other nations and international agencies (such as Interpol) is essential for exchanging intelligence and organising cross-border investigations, especially when transnational cybercrime is involved.

Technological Actions:

Development of cybersecurity infrastructure: It is essential to invest in the nation's cybersecurity infrastructure. This include creating safe government networks, enhancing the capacity of the national CERT (Computer Emergency Response Team), and raising awareness of cybersecurity among individuals and organisations.

Materials.

Threat intelligence and detection: It's critical to use cutting-edge technologies for threat identification and reaction. This may entail using artificial intelligence (AI) for threat analysis, security information and event management (SIEM) platforms, and advanced intrusion detection systems.

Digital forensics: To investigate cybercrimes, retrieve evidence, and bring offenders to justice,

strong digital forensic capabilities are necessary. Uzbekistan probably spends money on instruments and training for professionals in digital forensics.

Blockchain technology: By improving the traceability of digital assets and enhancing the security of various online transactions, blockchain's built-in security features may be used to support investigations.

Education and Public Awareness:

Campaigns to raise awareness about cybersecurity: Campaigns to raise public awareness about malware, phishing schemes, safe online practices, and online safety are essential. These initiatives lessen people's and organisations' susceptibility to cyberattacks.

Education and training: To increase capacity and enhance abilities in effectively combating cybercrime, training programs for law enforcement, cybersecurity experts, and the general public are essential. Difficulties:

Notwithstanding these initiatives, Uzbekistan still confronts a number of obstacles:

Restricted resources: It takes a large financial commitment and specialised knowledge to build a strong cybersecurity infrastructure and train personnel, both of which may be scarce in some places.

Research and methods.

Threats are always changing because cybercriminals are always coming up with new strategies, which makes it difficult to keep up with them.

Cybercrime's cross-border character: While international collaboration is essential, coordinating investigations and prosecutions across many legal systems can be challenging.

Digital literacy: Raising the general public's level of digital literacy takes time and consistent work.

As of October 2023, Uzbekistan has made great progress against cybercrime by implementing a number of contemporary tactics and procedures. Here are a few crucial methods:

1. Legislative Framework: In order to better combat cybercrime, Uzbekistan has been creating and revising its legal framework. This entails passing legislation that clarifies what constitutes a cyber offence, stiffens the penalty for cybercrime, and creates procedures for inquiry and prosecution.
2. National Cybersecurity Strategy: To improve the general security of the nation's cyber infrastructure, the government has put in place a national cybersecurity strategy. This entails raising awareness, encouraging global collaboration, and safeguarding vital information infrastructure.
3. Creation of Cybersecurity Agencies: To improve the government's capacity to stop and address cyberthreats, specialised cybersecurity agencies have been established, such as the Ministry of Digital Technologies' Cybersecurity Centre.
4. Public Awareness Campaigns: To inform businesses and citizens about cyberthreats and safe online habits, the government and a number of non-governmental organisations run awareness campaigns. These initiatives support the development of a cybersecurity culture.

Discussion.

5. Capacity Building and Training: To help law enforcement, the court, and other stakeholders become more adept at managing cybercrime matters, Uzbekistan funds training initiatives. This involves working together internationally with nations and organisations that have cybersecurity expertise.
6. International Cooperation: Uzbekistan works with regional partnerships, the United Nations

Office on Drugs and Crime (UNODC), and international organisations like INTERPOL to successfully tackle cybercrime. This kind of collaboration facilitates information exchange and coordinated efforts to combat global cybercrime.

7. Technological Investments: To fight against any cyberthreats, the government has been spending money on cutting-edge technology and cyberdefense measures like intrusion detection systems and sophisticated data security techniques.
8. Collaboration with the Private Sector: Given that many cybersecurity threats impact businesses, it is imperative to engage with private sector firms. To strengthen the country's cybersecurity posture, the government promotes collaborations with tech and cybersecurity companies.
9. Creation of Cybercrime Units: Within law enforcement organisations, specialised units are dedicated to looking into cybercrime. These teams have the knowledge and resources needed to manage intricate digital investigations.
10. Incident Response and Recovery Plans: It's critical to create and carry out incident response plans in order to promptly handle and lessen the impact of cyber incidents. This includes updating response tactics and conducting frequent drills.

Conclusion.

These techniques show Uzbekistan's dedication to building a robust cybersecurity ecosystem to safeguard the nation's digital environment. As cyber dangers become more sophisticated and complicated, further upgrades and reforms are anticipated.

In summary, Uzbekistan's strategy for fighting cybercrime is probably a multifaceted one that combines public awareness campaigns, technology advancements, regulatory frameworks, and international collaboration. But the details are still mostly unknown, and it's still difficult to tell if these steps are working.

List of used literatures:

1. Constitution of the Republic of Uzbekistan, adopted on December 8, 1992.
2. Criminal Code of the Republic of Uzbekistan, as amended (1994).
3. Code of Criminal Procedure of the Republic of Uzbekistan, as amended (1994).
4. Law of the Republic of Uzbekistan on Combating Corruption, adopted on January 3, 2017.
5. Law of the Republic of Uzbekistan on Combating Trafficking in Persons, adopted on April 17, 2008.
6. Law on Prevention of Delinquency, adopted on August 29, 2014.
7. United Nations Convention against Transnational Organized Crime, 2000.
8. United Nations Convention against Corruption, 2003.
9. Commentary on the Criminal Code of the Republic of Uzbekistan, edited by legal experts of Tashkent State University of Law.
10. International Treaties of Uzbekistan on Crime Prevention, Ministry of Justice of the Republic of Uzbekistan.