Improving International Cooperation on Combating Cybercrime

Bakhodirov Domullojon Baxtiyorzoda
Tashkent State University of Law
bakhodirovdadakhon@gmail.com

Abstract

In today's informed world, cybercrime makes a substantial contribution to crime. As a result, this article discusses research methodology, the establishment of international cooperation in the disclosure of committed crimes, the existing difficulties in the collection of electronic evidence, the lack of single, universal treaties in the fight against them, and the need to develop such a treatment.

In this article, I have described the need for a global integrated system, as well as the procedure for carrying out the necessary actions for its implementation, by researching cybercrime conventions and agreements on mutual legal assistance in the country.

Key words: cybercrime, international cooperation, combating cybercrime, Budapest convention, International Treaties and Agreements, Enhanced Information Sharing

I. Introduction

It is recognized that we are living today in the era of information and communication technology, which has become the basis on which all fields depend on, and with all institutions, whether it is public institutions owned by state governments or private institutions owned by individuals, the information technology is the tool for managing the affairs and networks. Countries and the provision and facilitation of services through them. [1] The digital environment has turned into a haven for cybercriminals in our increasingly linked world, who take advantage of weaknesses to gain financial advantage, conduct espionage, or compromise vital infrastructure. The sophistication and tactics of cyber assaults are evolving along with technology, underscoring the pressing need for more international collaboration in the fight against this worldwide threat. In order to protect the digital sphere, this article examines the difficulties posed by cybercrime

and promotes increased international cooperation.

Cybercrime has no borders, with criminal actors operating across borders to exploit vulnerabilities in digital systems. Cyberattacks have enormous financial consequences, with billions of dollars lost each year due to ransomware, identity theft, and fraud. Furthermore, the growing prevalence of state-sponsored cyber-espionage poses a serious threat to national security. The financial loss caused by cybercrime was projected at US$ 1.5 trillion in 2018, and it was expected to climb to US$ 2 trillion by the end of 2019, and US$ 6 trillion by 2021. Understandably, government and corporate investment on cyber security is increasing.[2] Information such as this necessitates the establishment of a single, global partnership for cybercrime within the global community.

II Methodology

This article outlines a process for forging a common framework among states to improve their collaboration on cyber security. In the other hand effective international cooperation in the fight against cybercrime is hampered by a variety of issues. These issues include disparities in state-to-state technology capacities, complex jurisdictional issues, and many legal foundations. Furthermore, issues with data privacy and sovereignty frequently obstruct the transmission of critical information required for an expedient reaction to cyber disasters. Creating a single interactive collaboration is one of the issues in this article that has to be resolved like development standardization of Cybercrime laws, enhanced information sharing, capacity building, setting-off public-private partnerships, creating international reaties and agreements.

Additionally, we have to examine the international cooperation methods and procedures that align with the specific characteristics of cybercrimes and need prompt reactions that occur. These crimes have a connection to information networks. The collaborative character of national legal systems inside one another.

III Result

The evaluation of current International cooperation on cybercrime leads to essential events like transborder system of cybercime law with the help of advancing among all countries of world and it causes to improve mutual contact together. The fact that cyber interactions that are risk-free can result in bottlenecks:

First and foremost, to the prosperity of large-scale socioeconomic connections, acquiring state collaboration;

Second, the achievement of secure personal data storage,

Third, a diverse spectrum of online financial resources circulates freely in the global trade sector.

Fourth, because of the existence of a single interactive system, emerging countries can attain specific goals, such as achieving rapid growth in successive years and attracting substantial quantities of investment dollars.

Fifth, shared collaboration allows states to easily trace down and identify criminals, expedite the acquisition of information about their IP addresses, and build cooperation on extradition concerns.

Sixth, as a result of the formation of electrons in the collection of evidence

IV Discustion

1. Creating general International Treaties and Agreements

To encourage international collaboration in the fight against cybercrime, a number of treaties and accords have been developed. The objectives of these accords are to tackle the difficulties presented by worldwide cyber threats and encourage cooperation. But there is no international convention on struggling cybercrime among the countries of the world(there is some regional convention such as Budapest convention, African Union Convention on Cyber Security and Personal Data Protection, ASEAN Convention on Cybercrime (2015), Shanghai Cooperation Organization (SCO) Agreement on Cooperation in the Field of International Information Security (2009) etc).

The third chapter of the Budapest Convention, which was approved on

November 23, 2001, deals with international cooperation among parties in cybercrimes. In the article of 23 of convention is said The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.[3] It is clear that all member countries collaborate in the area of investigations or proceedings pertaining to criminal offenses related to computer systems and data, or for the collection of electronic evidence of a criminal offense. On the other hand it is only among EU parties. For example, if someone is not a citizen of an EU state, they may have attacked the personal information of EU members, obtained their personal information, and taken money from the account. In this instance, the states must gather information, share it, and decide what steps to take in order to locate the offender. Since the act's perpetrator is a citizen of a nation that is not a party to the Budapest Convention, it is unclear what responsibility the nation bears under this legislative standard. Wojciech Wiewiórowski, EDPS, said: “Exchanging personal data between EU countries and non-EU countries to combat cybercrime comes with great responsibility. Strong safeguards must be put in place to ensure that the protection of individuals’ personal data in a non-EU country is not undermined, especially when sharing sensitive data related to alleged criminal activities. [3]

Therefore, it is important to form agreements and treaties that will benefit all countries in the globe and foster mutual cooperation between them in order to prevent such misunderstanding.

A variety of actions must be taken in order to get such results. For instance,

a) Standardization of Cybercrime Laws

That is, it is imperative to establish a unified framework for the definition and prosecution of cybercrime. The goal of harmonizing laws pertaining to

information exchange, extradition, and cyber offenses should be pursued by nations. A globally recognized legal framework would make cooperation and extradition procedures run more smoothly. [5] The process of setting up and putting into effect uniform legal structures to address cybercrimes across various jurisdictions is known as "standardization of cybercrime laws." Standardized regulations are becoming more and more required as technology improves as a way to safeguard coordinated and productive responses to cyberthreats.

b) Enhanced Information Sharing

For organizations to effectively tackle cybercrime, increasing information sharing is essential since it enables stakeholders to communicate threat intelligence, event data, and best practices in real time. Establish safe and reliable channels for information sharing on emerging threats, vulnerabilities, and attack patterns between governments.These systems ought to make it easier to collaborate in real time while protecting the privacy of shared data.

c) Capacity Building

Collaborate to develop and implement joint training programs that bring together international law enforcement, legal experts, and cybersecurity specialists. These courses can cover a variety of topics, including digital forensics, incident response, and international legal frameworks. Promote international cybersecurity specialists to exchange best practices, insights, and knowledge. To cooperate and exchange expertise, professionals can form joint task teams, collaborate on projects, and be sent on secondments. Organize and participate in international workshops and conferences on cybersecurity. These events provide a venue for networking, knowledge sharing, and discussions about recent advancements and challenges facing the sector.

The international community must continue to be dedicated to assisting nations in enhancing their ability to combat cybercrime. Cooperation, resource sharing, and advancement can help countries better address the global and dynamic character of cyber threats.

Conclusion

This article has explored enhancing global collaboration to fight cybercrime with the help of some measures such as establishing broad international greements and treaties It is clear that, despite the fact that the international community recognizes that law harmonization and international cooperation are critical to achieving global cyber security, the international community has yet to finalize a universal comprehensive code to combat cybercrime, owing to differences in national approaches to such harmonization. Extradition, reciprocal legal assistance, mutual recognition of foreign decisions, and informal police-to-police cooperation are all examples of international cooperation today.

However, due to the volatile nature of electronic evidence, international cooperation in criminal issues in the area of cybercrime necessitates prompt replies and the capacity to seek specialized investigative procedures, such as computer data preservation. Therefore, it is important that Cybercrime Legislation Standardization, Improved exchange of information, international capacity development are the most important way to achieve nationally single system to figting global cybercrime.

References

1. INTERNATIONAL EFFORTS TO COMBAT CYBERCRIME Dr. Baqer Musa Saeed AL_khafagy Department of Law, College of Law, The Islamic University, Najaf, Iraq PJAEE, 17 (6) (2020) file:///C:/Users/User/Desktop/Digital%20forensic/ariticle%203.pdf

2. INTERNATIONAL COOPERATION IN FIGHT AGAINSTCYBER-CRIME ByBrigadier Saurabh TewariCentre for Joint Warfare Studies Kashmir House, Rajaji Marg, New Delhi-110 00 3 PRESS RELEASEEDPS/2022/14 file:///C:/Users/User/Desktop/Digital%20forensic/aqrticle%202.pdf

3. Brussels, 20 May 2022 “A new United Nations convention on cybercrime: fundamental rights come first” https://edps.europa.eu/system/files/2022-05/EDPS-

2022-14-A%20new%20United%20Nations%20on%20cybercrime-fundamental%20rights%20come%20first_EN

4. Convention on Cybercrime Budapest, 23.XI.200 https://rm.coe.int/1680081561

5. RELEVANCE OF INTERNATIONAL LAW IN COMBATING CYBERCRIMES: CURRENT ISSUES AND AALCO'S APPROACH Prof. Dr. Kennedy Gastorn∗ Secretary General of Asian-African Legal Consultative Organization (AALCO) Presentation at the 4th World Internet Conference, Wuzhen Summit, on the Session on "International Cooperation in Countering the Use of Cyberspace for Criminal and Terrorist Purposes", 4th December 2017, Wuzhen, China RELEVANCE OF INTERNATIONAL LAW IN COMBATING CYBERCRIMES: CURRENT ISSUES AND AALCO'S APPROACH Prof. Dr. Kennedy Gastorn∗ secretary General of Asian-African Legal Consultative Organization (AALCO) Presentation at the 4th World Internet Conference, Wuzhen Summit, on the Session on "International Cooperation in Countering the Use of Cyberspace for Criminal and Terrorist Purposes", 4th December 2017, Wuzhen, China. file:///C:/Users/User/Desktop/Digital%20forensic/article%204.pdf

6. Resolution 26/4 Strengthening international cooperation to combat Cybercrime The Commission on Crime Prevention and Criminal Justice, file:///C:/Users/User/Desktop/Digital%20forensic/aritcle%201.pdf