**ON COMBATTING CYBER CRIMES IN MONGOLIA: CURRENT CIRCUMSTANCE AND LEGAL FRAMWORK**

**Mungunshagai, Garaajav**

*Police captain*

*Dean of Department of Criminal procedure*

*Police School*

*Law Enforcement University, Ulaanbaatar, Mongolia*

***ABSTRACT:*** *Recent years have witnessed growing research interest in cybercrime in Mongolia. Being developing country in the list of Global Innovation Index finds is hard to catch up with other leading in cyber security and technology. However, leading countries including US, Russia, China, and UK etc are not safe from cyber-crimes and cyber-threats they face then how Mongolia can be considered safe against cyber-crimes. This type of crime requires all of the nations have to work together on this issues. The purpose of this study is introduce current circumstance and legal framework of cybercrime in Mongolia. Most of this research focused on legal framework on this crime. There is a research focused on current circumstance of this crime. In Mongolia, the issues of cybercrime regulated by the Constitutional Law, Criminal Law and Criminal procedure law have been the main focus, so that there is little research to improve on Combatting Cybercrime, Legal framework of cybercrime, and effectiveness of laws.*

***Keywords:*** *Cybercrime, Mongolia, Current circumstance, on Combatting cybercrime, Legal framework*

1. **INTRODUCTION**

In recent times, our society is increasingly relying on the internet and other information technology tools to engage in personal communication and conduct business activities among the other several benefits. The term cybercrime can be used to describe any criminal activity which involves the computer or the internet network. This term is used for crimes such as fraud, theft, blackmail, forgery, and embezzlement in which computers networks are used.

In 1996, first the internet service was launched in Mongolia since then over 20 years have been passed and the number of internet users have been growing constantly. With the population of Mongolia placed at 3.1 million from the last census carried out in 2018, a recent statistics revealed that about 64.1% have access to the internet which is very high percentage in the globally. In other words, two out of three people access the internet. By comparison, the internet users have been increasing drastically by 22% since a decade (Internet world stats, 2017).

According to the Internet world stats indicates that in 2000, there was 30000 internet users in Mongolia. By 2018, over 2.500.000 internet users in Mongolia3. Mongolians live in a connected world by internet. In addition, the use of the internet for facilitation of the work between individuals and organization have been increasing drastically (The Internet world stats, 2018). For instance, the number of online clients of banks from the 1st quarter of 2017 was 1.122.833 (Report of Bank of Mongolia, 2016). There are 110 public service e-kiosks operating around the country and people receive 34.073 inquiries and services per day (Report of the National Data Center 2017).

The international Telecommunication Organization assessed the ICT development indices of 166 countries by 11 indicators such as stationary and mobile telephones, computers, and internet access per 100 people in January 2017. Iceland was in the lead with 8,98 scores while Mongolia was on 91 nd place with score 4,96 (Report of The International Telecommunication Organization, 2017).

 For Mongolia, the number of Fixed-telephone subscription points per 100 inhabitants is 7.60, the number of mobile-cellular phone telephone users is 113.63, Percentage of individuals using the internet is 22.27, International internet bandwidth per Internet user is 166055.85mbit/s, Percentage of households with computer is 23.59, Percentage of households with Internet access are 23.57%, and Fixed (wired)-broadband subscription per 100 inhabitants is 7.63, Active mobile-broadband subscriptions per 100 inhabitants is 82 as reflected in the website of the Mongolian CITA (Report of Communication and Information Technology Agency, 2017). This indicates that the usage and service of ICT are the global level in Mongolia.

The Internet and information communications technologies have broken down geographical barriers, have brought together and created opportunities for economic growth and innovation. It has also created an opportunity to deliver service, transact business, and communicate in cyberspace for everyone. On the other hand, it has also provided opportunities for those with criminal or hostile objectives. The scale, speed, and global nature of cybercrime present a challenge to traditional law enforcement methods and skills, and to confidence in our online world.

To strengthening the legal frame work for better protection and prosecution, carry out prevention and awareness raising activities. The primary interest of this study is in determining and introducing overview of cybercrime in Mongolia. In order to overview of cybercrime tried to determine general condition and circumstances of cybercrime in Mongolia and legal Frame work for Combating Cybercrime such as Criminal law on combatting cybercrime, the National security concept of Mongolia, and the National Program on Information Security of Mongolia.

1. **GENERAL CIRCUMSTANCES OF CYBERCRIME IN MONGOLIA**

Cybercrime is a new trend that is gradually growing as the internet continues to penetrate every sector of our society. The notion of cybercrime can be very wide and the extent of the cybercrime problem is not well understood. About the cybercrime, we understand such crimes may be divided into one of two categories. The cybercrimes that affects computer networks and devices directly such as malicious code, computing viruses, and malware and crimes facilitated by computer networks or devices, the primary target of which is independent of the computer networks or device such as Cyber Stalking, fraud, identity theft, phishing. Presently, cybercrimes are performed by people of all ages ranging from young to old, but majority of instances the young. We are only seeing the tip of the iceberg for cybercrime.

The following are some common cybercrimes which we are dealing with.

* 1. Cybercrime in the Banking Sector: as the security level in this sector becomes stronger, the strength, and tactics of these fraudsters increases. Various lucrative attacks have been launched and unfortunately, many have succeeded. In general, cybercriminals execute fraudulent activities with the ultimate goal of accessing a user’s bank account to either steal or transfer funds to another bank account without rightful authorization.
	2. Phishing: which is simply the theft of an identity. It involves stealing personal information from unsuspecting users. Phishing scams are exponentially increasing. It has become one of the fastest growing cybercrimes in Mongolia.
	3. Intellectual Property Theft: the term Copyright means little or nothing to the average Mongolians. Piracy involves the unlawful reproduction and sharing of application software, games, movies, videos, and audios. The Internet has created a platform for almost anonymous, free and illegal distribution of pirated materials in Mongolia.
	4. Cyber-pornography: it is the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials, especially materials depicting children engaged in sexual acts with adults. Cyber-pornography is a criminal offense, classified as causing harm to person.
	5. Social media sector: In Mongolia, social networks have gained a very high ground in every sector. The banking industry, government, business, universities use this platform to promote and communicate with each other. Social networking sites such as Facebook, Twitter, LinkedIn, and Instagram serve as a fertile ground for cybercriminals to launch new attacks.
	6. Cyber-Stalking, harassment: threatening and blackmailing acts carried out on the internet by fraudsters on the victim. In most cases, the perpetuator’s identity is unknown by the use of false alias or by blocking the identity by keeping all information hidden.

In recent years, there has been increase in cybercrimes. Therefore, it is necessary to make the jurisdiction of cybercrime and traditional crimes occurring in online settings clear, to bring the terminologies into order, to raise awareness of public concerning online security, to increase preventive actions and increase the number of professional qualified manpower and human resources. According to the National Police Agency report indicates that there were 362 cases reported in 2017 and 409 cases in September of 2018 which is three times greater than 2016 in which 136 cases were reported (Report of National Police Agency, 2018). As for as complaints about cyber security and technologies, the National Police Agency received 395 complaints about it in 2016, the numbers have increased in 2017 as 416 and at September of 2018, the numbers of complaints increased drastically as 547(Report of National Police Agency, 2018). It is obvious that the numbers of cybercrimes case and the numbers of complaints of cybersecurity will increase even more.

Unfortunately, as of recent years, most of cybercrimes are committed and reported in the forms of other traditional crimes. For instance, if somebody wants to steal money from the E-bank by using internet, it would be investigated as larceny or theft. Committing cybercrimes are hidden ways, it is impossible to make a direct conclusion on the growth or reduction of such cases based only on registered crime statistics. Although there is some progress in a legislative and legal environment on protection of human rights of cybercrime victims, due to many hidden or traditional nature of crime cases are brought to the court which is fewer because the majority of cybercrimes have not been categorized as a criminal offense. The most cyber-related cases to be dismissed before court procedures. In addition, minority of people report cybercrimes and most organizations, entities, and offices conceal the fact about cyber-attack which have been faced. They are more likely think that they would lose credibility by announcing that their database is no longer secure.

In real world in Mongolia, specialists estimate that there would be five to ten times more cases of cybercrime than the currents statistics. It would be averagely 2.000 serious cyberattacks are committed annually in Mongolia and just 400 of them are reported to the police. It is also necessary to mention that in Mongolia, there are many instances of cybercrime go unreported. In some instances, victims will be unaware they have been affected. Some victims are too embarrassed to report the crime, do not know to whom to report, whether a crime has been committed, or do not believe law enforcement can provide a remedy. Experiencing a cyber-security breach would be high. This is not yet reflected in reporting, as Mongolia does not have a single, central point of reporting and breach disclosure is not mandatory. Even if they want to, victims do not always know where to report. Different agencies are responsible for different types of cybercrime, so some incidents will be reported to multiple places, while other victims may be passed from one agency to another in an effort to find the best place for a resolution. We will need to a better understanding of what is required to effectively combat cybercrime.

It is difficult to detect, investigate, and prosecute cybercrimes in Mongolia. This type of crimes can also be distinguished from traditional crimes by the challenges its global nature presents for law enforcement. In some case, individuals and groups overseas can operate wherever an Internet connection is present. The perpetrators are based overseas and are highly organized. One United Nations report estimates that 80% of cybercrime is part of organized criminal activity (The United Nations Report, 2014). Traditional organized crime groups are migrating to this environment for greater profit at less risk. The element of such a crimes make it difficult to find the perpetrator and access related evidence. Information exchange and cooperation between different countries can be poor and even where strong cooperative relationships exist, mutual legal assistance treaty processes can be very slow. Cases may require a disproportionate amount of investigative effort, reducing the availability of resources to deal with other demands. Moreover, the laws and regulations of Mongolia stay behind the rapid technological development. There has been lack of mutual understanding about the cybercrime at all level of the law enforcement agencies as well as General Prosecutor’s office and Supreme court.

1. **MONGOLIA’S LEGAL FRAMEWORK FOR COMBATING CYBERCRIME**

In 1992 Mongolia adopted a new Constitution, ensuring fundamental rights of Mongolian citizens, including the right to life, to freedom of religion, to free expression of opinion, to be free discrimination, and to freedom movement. It also establishes the right to free choice of employment, to favorable work conditions, and to be free forced labor (Constitution of Mongolia, 1992). In addition, the Constitution provides that all international treaties to which Mongolia is a party shall be effective.

For the Information security, according to the Cybersecurity Department of the General Intelligence Agency of Mongolia states that in the February of 2016, five countries have made cyber-attacks attempts frequently. Individuals or other groups of China attempted cyber-attacks 18.405 times, 4.536 attacks were recorded from the USA, Russia made 1.143 cyber-attack attempts, 869 from Taiwan and 621 from South Korea (Report of Cybersecurity Department of the General Intelligence Agency of Mongolia, 2016). Clearly, Mongolia’s two neighbors tremendously try to access information and database in Mongolia. The government of Mongolia viewed that in such conditions spread of information security might present high risk of negative effect on national security. In order to coordinate social relationships emerging in relation to activities on combating cybercrimes and its prevention in Mongolia, number of activities were implemented in such field as creating legal environment to joining protocols that determined norms and standards at international levels, ratification of declaration, making agreement on cooperation, allocation of budget, formation of an accurate understanding among general public. For example, in 2010, the National security concept of Mongolia was amended as “protection of national interests in the information sector and ensuring information integrity, confidentiality and access of governmental and private entities and individuals is the basis of information security”1. It officially became one of parts of the National security concept. The function of national security consists the State Great Khural of Mongolia, President of Mongolia, and the Government of Mongolia as well as National security council. Besides these, Cybersecurity Department of the General Intelligence, Unit of Combatting on cybercrime in National Police Agency, Special purpose military unit of General staff of the Armed force, and State budget Enterprise for Governmental digital data and information security are responsible to ensure national security. As result of National Program on Information Security was approved by Resolution #141 of the 2 June of 2010 to implement several activities such as instituting a unit for cybercrime and building relevant capacities (Resolution of Government of Mongolia, 2010). Unit of Combatting on cybercrime in the National Police Agency was created to prevent, investigate and respond to cybercrime. This step made a real contribution to prevention of cybercrime and protection of rights of citizens, business, and Government. This unit is the core Police unit that deals with cybercrime and provides Police with a central point of contact for other agencies. The unit has comprised of mix of detectives and technical investigators.

To mentioning other implementation of governmental resolutions and programs are Program Digital Mongolia 2005-2012, Program Digital Governance 2012-2016, Government Resolution on Integrated System of Comments in Websites 2013, and Program for facilitation of Foreign Trade 2007, as well as State policy on the development of the information and communications technology /2017-2025/ which are indicative of the level the current development of the society. In addition, more than 10 communication and information security standards have adhered in Mongolia. However, a number of questions need to be resolved and paid attention to for successful implementation of program and further work. There is lack of research and surveys that examine causes and circumstances for cybercrime. It is also critical to focus on development of a legal framework that would cover all aspects of security in the information space including the traditional information media such as conversation, information exchange, advertisement, trade, training, surveys, press, books and magazines. Basically, the legal regulation for cybercrime gradually improved since then. Although an independent law hasn’t been established for cybercrime which makes uncertain ways to Agencies and authorities in charge of ensuring information security do not know what they are supposed to do or how they should operate due there is not an independent law.

Regarding the Criminal Law of Mongolia: The criminal law is the central piece of legislation in Mongolia’s criminal justice system, and it is the only law that carries prison sentences for violations. Over the years, Mongolia’s Criminal law has been amended to better address cyber offences. For instance, the Criminal law of 1998 categorizes crime against information security in Chapter 5, crime against security of computer information in Chapter 25 in the Criminal law of 2002 and as crime against security of digital data in Chapter 26 of the new edition of 2015 of the Criminal law.

As for as the new edition of 2015 of the Criminal law, the name of the Crimes Against the Security of Computer Data Chapter of the Criminal Law has been changed as linked to digital services. In other words, the law and regulation have improved relatively. In particular, the new edition can hold 14-year-old accountable if they illegally access digital information and create, use, sell and distribute any harmful software or hacking programs and technology.

 **VI. CONCLUSION**

Despite improvement to Mongolia’s legal frame work, Mongolia continues lack comprehensive anti-cybersecurity legislation. Cybercrime became officially one of controversial issues in worldwide and fighting alone is impossible. Globally, nations are required to establish a cooperation agreement or join a convention related to cybercrime, to coordinate and link them, to create opportunities for implementation mechanism to work fully in Mongolia, which will give an opportunity to understand terms used in conventions in one way at national level.

In addition, expanding cooperation and cooperating with other nations can be crucial to improve our ability to prevent, investigate, and respond to cybercrime and reduce harm to the citizens of Mongolia.

Most importantly, this new trend of crime should be eradicated or reduced to a very minimal level for worldwide. Many numbers and incidents show that majority of the cybercrimes conducted are carried out by the youths in our society majorly through phishing. There is need for them to be oriented, educated and empowered for the country to have a greater future.

REFERENCE,

Communication and Information Technology Agency : <http://cita.gov.mn/>

The National Police Agency, Annual Report, 2018

The General Intelligence Agency of Mongolia, Department of Cybersecurity, Annual Report, 2016.

Government of Mongolia, Resolution #141, “National Program on Information Security”, 2010.

Report of Bank of Mongolia 2017

Report of National Data center <https://datacenter.gov.mn/service/tutsmashin> 2017

<https://www.internetworldstats.com/stats.htm>

<https://www.internetworldstats.com/>

<https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2017/methodology.aspx>

United Nations Office on Drug and Crime “Comprehensive Study on Cybercrime: Draft. (February 2013). Last accessed: http://www.unodc.org/documents/organized-crime/UNODC\_CCPCJ\_EG.4\_2013/CYBERCRIME\_STUDY\_210213.pdf