Pax Mongolica №4, 2016: 104-123 pages

Is Mongolia Ready to Join Budapest Convention on Cybercrime?

Bat-Amgalan Turbat*

Abstract: *It is not right to consider that cybercrime which contains transnational features is not a subject to jurisdiction of any given country for it possesses power to inflict damages to infrastructures of more than one nation. Therefore, it has become essential to have active multilateral cooperation in international law in order to conduct efficient fight against cybercrime requires*[1]*. In such circumstances, Mongolia is required to have active participation in the international cooperation to provide safety measures or security system on cybercrime, too. And the legal basis for the multilateral cooperation of cyber security is the Budapest Convention on Cybercrime which allows non-European Union member states to join. There are 21 member states (parties) outside the European Union in the Convention, so far*[2]*.*

Keywords: *Budapest Convention on Cybercrime (aka Budapest Convention or Convention on Cybercrime), Council of Europe, cybercrime*

Introduction

In Mongolia, fight against cybercrime is regulated by criminal law. According to the articles 226-229, Chapter 25 - "Crimes Against the Security of Computer Data", Criminal Code of Mongolia, those who committed cybercrime are subjects punishable by a monetary fine or incarceration

* Ph.D Candidate, Researcher at the Department of International Law, Institute of International Affairs, Mongolian Academy of Sciences

[1] Transnational organized crime: the globalized illegal economy https://www.unodc.org/toc/en/crimes/organized-crime.html

[2] Article 37 - Accession to the Convention, Convention on Cybercrime; Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States. http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG

depending on the severity of their crimes[3]. And by the articles 26.1-26.3, Chapter 26 - "Crime Against the Security of Online Data", revised version of the Criminal Code of Mongolia that is to be effective from the September 1st, 2016, it is regulated how to ensure the security of online data against cyberattacks[4].

As provisioned in the article 2.1, Criminal Code of Mongolia, the criminal laws of Mongolia are to be in compliance with the Mongolian Constitution and commonly/universally recognized standards of international law. But, at present, in Mongolia the commonly recognized standards against cybercrimes are not followed. This is because we have not officially adopted the standards yet[5]. Therefore, having considered such issues, following research has been conducted regarding the possibilities/ opportunities for Mongolia to join the Budapest Convention on Cybercrime.

One. Will of Mongolians to Join the Budapest Convention on Cybercrime

In the Supplement#2 - "Implementation plan of the national programme for information security", the Government Resolution#141 passed in 2010, international legal regulation on cybercrime is reflected as follows[6]:

Implementation procedures and duration	Expected outcome	Implementation agency	Criterion
Join international conventions and treaties against cybercrime and develop foreign relations concerning this issue (2010-2015)	National information security is expected to be secured at international level	Central Intelligence Agency of Mongolia; Information Technology, Post and Telecommunication Authority (ITPATA); and Ministry of Foreign Affairs	Number of the international treaties Mongolia is member of

In 2010, the Mongolian government passed a resolution to join

[3] "State Information" pamphlet, №5, 2002, Criminal Code of Mongolia, 2002 https://www.unodc.org/res/cld/document/mng/2001/criminal_code_of_mongolia_html/Mongolia_Criminal_Code_2002.pdf

[4] "State Information" pamphlet, №7, 2016, Criminal Code of Mongolia (revised), 2016

[5] List of multilateral treaties Mongolia is member of - website of the Ministry of Foreign Relations http://www.mfa.gov.mn/?page_id=29040

[6] Supplement#2 - "Implementation plan of the national programme for information security", the Government Resolution#141, http://legalinfo.mn/annex/details/2687?lawid=4716

international treaties/agreements to fight cybercrime, and develop our foreign relations and cooperation regarding this issue. Unfortunately, since the resolution passed Mongolia has not yet managed to have any membership access to any international conventions[7]. However, the issue was not neglected completely for some measures were taken meanwhile. For example, Budapest convention has been translated at the Legal Institute of Mongolia[8], Cyber Security Agency experts have been enrolled in trainings or courses conducted by foreign expats[9] and various researchers have expressed their positions, publicly, saying that we should join the convention[10].

Furthermore, in the National Security Concept developed by the Mongolian parliament we said that "Bilateral relations and multilateral cooperation shall be continuously pursued in security and defense areas with Mongolia's two neighboring states, the USA, member states of NATO, the European Union and the Asia-Pacific region along with active participation in international peacemaking missions"[11]. As I see it, this provision applies to the fight against cybercrime as well.

Other important factor that urges us to join the convention is the international cooperation regulation on cyber security. In the articles 23-25, Chapter III, Convention on Cybercrime, cyber security is regulated at the international level by means of cooperation. Particularly in the article 23 which is about general principles relating to international cooperation it says that "the parties shall co-operate with each other 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, for the purposes of investigations or

[7] Chart of signatures and ratifications of Convention on Cybercrime. Status as of 01/04/2016 http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=ugbVoPun

[8] Convention on Cybercrime has been translated into 19 languages including Mongolian and published in the Euorpean Council website http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime ConventionOtherLg_en.asp http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_Mongolian.pdf

[9] "Dr. Alexander Seger, Executive Secretary of the Committee of the Parties to the Budapest Convention on Cybercrime, was invited to conduct training courses for judicial and law officers. At the end of the training 50 trainees enrolled (approximately) expressed their opinions and suggestions regarding the issue" by D. Altan, 2012.05.19 http://www.mminfo.mn/content/24974.shtml

[10] L.Galbaatar. Resolving a cybercrime case by a court (Training handbook for judges, prosecutors and investigators). NUM Press Publishing. Ulaanbaatar. 2015. p. 37

[11] Article 3.1.1.6, National Security Concept of Mongolia - supplement to the parliament resolution#48, 2010

proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence".

Also the article 25 says that "the parties shall afford one another mutual assistance for the purpose 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". And the article 35 which regulates issues related with network says that "each party shall designate a point of contact available on a twenty-four hour, seven-day-a week basis, in order to ensure the provision of immediate assistance for the purpose 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"[12].

In the articles 2-10, Budapest Convention, cybercrime is divided into following four categories:

1. Offences against computer data, network privacy and proper use
2. Computer crime
3. Offences related to inappropriate cyber content
4. Offences related to infringements of copyright and related rights

Following subjects are mainly violated by the offences mentioned above:

1. Computer data or network
2. Computer, computer system
3. Morally appropriate content
4. Copyright and related rights

So it is seen that the rights protected by the convention or, in other words, objects of the offences and crimes mentioned above are computer data, network privacy, proper usage of network, online content, right and safety of children/family, cyber security of social life and copyright. Furthermore, one can reach a conclusion that cybercrime is to be divided into two sub-categories of "crimes/offences against computer and network"

[12] Chapter III - International co-operation. Convention on Cybercrime. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

and "crimes/offences committed by misuse of computer, information technology and other devices".

Because there are no specialized separate provisions or articles regarding crimes/offences committed by intentional misuse of computer and information technology devices in the Criminal Code of Mongolia, it can be considered that in Mongolia regulation on cybercrime is not legalized to the satisfactory extent.

Having concerned everything said above, it is plainly seen that there is a stern need for Mongolia to join the Convention on Cybercrime. And even if Mongolia becomes a party of the convention, our judge, prosecutor and inspector must be prepared to follow the convention provisions in compliance with judicial system[13][14].

Two. Opportunities for Mongolia to Join the Budapest Convention on Cybercrime

Budapest Convention on Cybercrime was adopted by the Committee of Ministers of the Council of Europe at its 109th Session[15] on in Budapest, Hungary on 2001.11.23 and entered into force on 2004.07.01[16]. Today, there are 45 nations ratified the convention and 8 nations signed it but not ratified.

Even when it was founded by the Council of Europe, it is allowed to have non-EU member states as a party of the convention, according to the article 37[17]. In particular, 21 nations not member of the Council of Europe are included in the parties[18].

---

[13] Article 10.3, the Mongolian Constitution: The international treaties to which Mongolia is a Party, shall become effective as domestic .legislation upon the entry into force of the laws on their ratification or accession

[14] Mongolian translation of the convention is attached with the supplement#1

[15] Explanatory Report. Convention on cybercrime, http://conventions.coe.int/Treaty/en/Reports/Html/185.htm

[16] Convention on Cybercrime. Budapest, 23.XI.2001
http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[17] Article 37 - Accession to the Convention

1. After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers

[18] Treaty open for signature by the member States and the non-member States which have participated in its

Table 2. Parties of the Convention on Cybercrime which are non-member of the Council of Europe nations

№	States	Signed date	Ratified date	Effective date
1	Argentina			
2	Australia		30/11/2012 a	1/3/2013
3	Canada	23/11/2001		
4	Chile			
5	Colombia			
6	Costa Rica			
7	Dominican Republic		7/2/2013 a	1/6/2013
8	Israel			
9	Japan	23/11/2001	3/7/2012	1/11/2012
10	Mauritius		15/11/2013 a	1/3/2014
11	Mexico			
12	Morocco			
13	Panama		5/3/2014 a	1/7/2014
14	Paraguay			
15	Peru			
16	Philippines			
17	Senegal			
18	South Africa	23/11/2001		
19	Sri Lanka			
20	Tonga			
21	United States of America	23/11/2001	29/9/2006	1/1/2007

As seen in the experience of previous years, having discussed with its parties, the Committee of Ministers of the Council of Europe invites a non-member state of the council to join the convention as a party upon the voluntary request of the nation to have accession. However if any of the

elaboration and for accession by other non-member States. http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG

present parties veto the request, the Committee of Ministers is to deny the grant of accession. But, in theory, the veto by a present party which is not a member state of the Council itself, has no impact on decision of the Council.

Although it looks like that request by the non-member state of the Council to join the convention is hugely dependent on the convention parties, final decision to grant accession right is made by the parties that have seats in the Committee of Ministers of the Council of Europe. As said in the Article 20.d of the Statute of the Council of Europe the request is approved with the decision of majority (two thirds of the parties) and also unanimous decision by the member parties of the Committee[19].

Therefore to be a party of the Convention, the present 45 parties should support the request of Mongolia. The fact that Mongolia hosted "5th Asia Pacific Telecommunity Cybersecurity Forum" in May 2014 and "5th Freedom Online Conference" in May 2015 is an actual expression of our utmost will to fight cybercrime and ensure cyber security. Such active participations also play positive roles in our effort to be a party of the Convention on Cybercrimes[20].

And again I personally believe that "5th Freedom Online Conference" held in Mongolia on May 4th-5th, 2015 will pay and contribute greatly in our willingness to join the Convention, because the Freedom Online Coalition which has 29 member states[21] so far was chaired by Mongolia during 2014-2015[22]. Members of the coalition are Australia, Austria, Estonia, Canada, Kenya, Costa Rica, Ghana, Georgia, Germany, Ireland, Japan, Latvia, Lithuania, the Maldives, Mexico, Moldova, Mongolia, the Netherlands, Norway, New Zealand, Poland, Finland, France, Czech, Spain, Sweden, Tunisia, UK and USA. Australia and Norway are the latest members. The coalition works in cooperation with numerous international or inter-governmental agencies/forums such as UN Human Rights Council,

[19] Accession to the Convention (Article 37). Explanatory Report. Convention on cybercrime http://conventions.coe.int/Treaty/en/Reports/Html/185.htm

[20] 5th APT Cybersecurity Forum (CSF-5), http://www.aptsec.org/2014-CSF5; Reflections on the 5th Freedom Online Conference in Mongolia, https://www.freedomonlinecoalition.com/news/reflections-on-the-5th-freedom-online-conference-in-mongolia/

[21] Today, 29 governments are part of the Freedom Online Coalition: https://www.freedomonlinecoalition.com/about/members/

[22] Costa Rica announced as next FOC Chair, https://www.freedomonlinecoalition.com/news/costa-rica-announced-as-next-foc-chair/

UNESCO, OSCE (Organization for Security and Cooperation in Europe), Digital Governance Forum, Stockholm Internet Forum and Global Partners Digital. And 20 members of the Freedom Online Coalition are the parties of the Convention on Cybercrime as well. And Ghana, Kenya, the Maldives and Tunisia, countries which are not member states of the Council of Europe, are not yet parties of the Convention.

But, more importantly, it can not be denied that the fact that our neighbors Russia and China are not parties of the Convention may have negative affect on the present parties' decision to put trust in Mongolia and support us to be a party.

Three. About Anti-Cybercrime Measures Taken in Mongolia

To be a party of the Budapest Convention on Cybercrime, we are required to give the present parties a certain picture of how issues related to cybercrime are legally regulated in Mongolia. Even more, if we become the party, we will have to update or amend our laws, rules and procedures. So in this part I have summarized the result of the research regarding how cybercrime is prevented in Mongolia.

3.1. Countermeasures against cyber attack

As said in the Supplement#2 - "Implementation plan of the national programme for information security[23]", the Government Resolution#141 passed in 2010, goals are to be achieved in Mongolia between 2010-2012: establish a specialized system in order to prevent from/react against incidents related to information security, cybercrime and cyber terrorism; develop and stabilize operational activity of the counter-cyberattack national team (MonCIRT) to the extent of CERT; and improve cooperation with international agencies that conduct similar operations (APSERT, FIRST, CERT/CC). As the outcome of the achievement, we will have our own professional cyber emergency response team that carries out technical complex tasks at international level.

Here I would like to make a little clarification - if one understands that the terms "countermeasure" or "response action" means only to

[23] Supplement#2 - "Implementation plan of the national programme for information security, the Government Resolution#141 passed in 2010, http://legalinfo.mn/annex/details/2687?lawid=4716

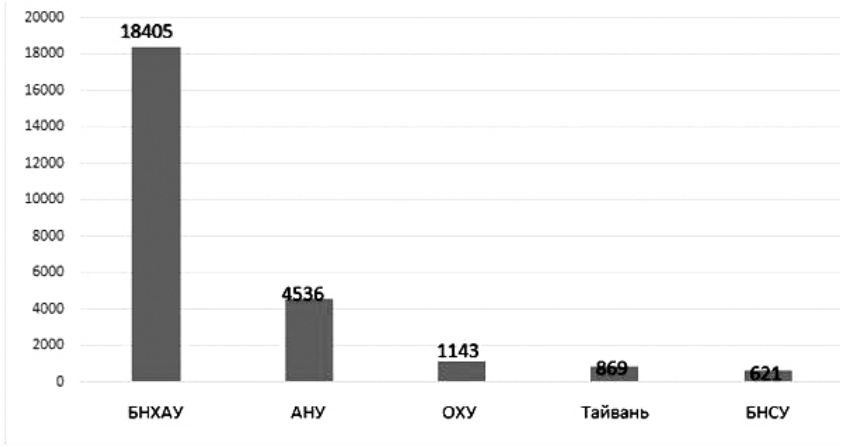
make cyberattack back, it will be too one-sided comment. This is because cyberattack consists of various harmful systems, programs and software such as botnet, logic bomb, Trojan horse, virus, worm, zombie etc[24]. Therefore it is morally wrong action to invent, use and disseminate programs specifically designed to have harmful viruses in the name of countermeasures against cyberattack.

In Mongolia, establishment of the cyberattack countermeasures systems is in the early stages of development. Today there is only one organization is running in this field - Cyber Emergency Response Team/ Coordination Center[25] (MNTCERT/CC) which was founded because there had been no controlled system to ensure cyber security and thus it had become priority to establish one. The MNTCERT/CC is responsible to:

- Find out cyber attacks in advance and take precautionary measures
- Conduct related trainings/courses
- Show 24/7 service to its members
- Provide professional counsels and warning notices

The study conducted on only 0.02% of Internet browsing in Mongolia and the in the following graphics showing total real-time accesses as of 2016 Feb and showing top 5 potential threats from overseas.

[24] Judicial General Council of Mongolia. Training manual for criminal law. p 115, Ulaanbaatar, 2015
[25] About MNCERT/CC - Cyber Emergency Response Team/Coordination Center http://mncert.org/about.php



1. 18405 - People's Republic of China;
2. 4536 - United States of America;
3. 1143 - Russian Federation;
4. 869 - Taiwan;
5. 621 - Republic of Korea

3.2. National legal regulation on cyber terrorism

In regard to the national regulation, my research has been based on Criminal Code of Mongolia, Law on Combatting Terrorism (Mongolia), Supplement#2 - "Implementation plan of the national programme for information security, the Government Resolution#141, 2010 and e-archive of the court orders.

Is "cyber terrorism" categorized as terrorism?

As defined by legislators and security researchers, cyber terrorism which includes any act that use information technology, computer system and e-communication as means of terrorism is categorized as one of cybercrimes[26]. Individual who commits such action is defined as cyber terrorist.

[26] Cyberterrorism definition http://searchsecurity.techtarget.com/definition/cyberterrorism

Is “cyber terrorism” a terrorist act?

As seen in the article 178 the Special part of the Mongolian criminal code and article 3.1.1, Law on Combatting Terrorism, terrorism is a concept that includes every type of terrorist acts. And since in the article 3.1.3.4, Law on Combatting Terrorism, attack on the social network for the purpose of terrorism is defined as terrorist act, cyber terrorism is legislatively categorized as one of cybercrimes.

How well is legal regulation against “cyber terrorism” developed in Mongolia?

In the framework of strengthening information security[27] and capacity of counter measures against cyberattacks following steps are to be taken: /2.3.5/ prevent from/react against incidents related to information security, cybercrime and cyber terrorism. In addition, to establish a system ensuring state information security, nest steps are to be taken: strength the capacity of fighting cybercrimes.

Therefore, having considered what is stated by the institutions mentioned above, I have come to a conclusion that, in the National Security Concept, cybercrime and cyberterrorism are defined as separate concepts however considered as the same subject for policy regulation.

3.3. National legal regulation on cybercrime

Following offenses legalised as cybercrimes in the articles 226-229, chapter 25, criminal code:

- Article 226. Alteration, damage or destruction of the computer data or software
- Article 227. Illegally obtaining of the computer data
- Article 217. Preparation and sale of devices for illegally entering the computer data network
- Article 229. Designing, using or dissemination of a computer virus

[27] National Security Concept of Mongolia, 2010 http://www.nsc.gov.mn/sites/default/files/images/National%20Security%20Concept%20of%20Mongolia%20EN.pdf

And elements of the offences are defined as follows:

- Tools of cybercrime
- Violation act
- Type of offence
- Material damage
- Legal punishment

Thus, according to the criminal code, offences defined as cybercrime are interpreted either as "with elements of material damage", "intentional", "severe" Tools, methods and applications used for the offences are:

1. Computer, program and other hardware
2. Data transmitted or stores in the computer and network
3. Protected computer and information network
4. computer data/information

Objects protected by the code are the information security of individuals and institutions. And by the code investigator from the intelligence agency and police inspector from the counter-cybercrime department execute investigations[28].

Cyber Security Department[29] was founded by the government resolution#312 (aimed to provide measures ensuring state information security) in 2011 to create protection for the state agencies from cyberattacks. However the department is not given right and power to execute investigation on offences against data security.

In the Supplement#2 - "Implementation plan of the national programme for information security", the Government Resolution#141 passed in 2010, countermeasures against cybercrime is reflected as follows:

[28] Criminal Procedure Law of Mongolia - article 26.3. Police agency shall execute investigation with respect to minor or other less severe crimes defined in article 26.2; article 27.4. Police agency investigator shall execute investigation with respect to severe or other extreme severe crimes defined in articles 27.1 and 27.3 http://www.oecd.org/site/adboecdanti-.corruptioninitiative/46816723.pdf 7.1

[29] Main page - "About Us", website of the Cyber Security Department, http://ncsc.gov.mn/?lang=mn&cat=1

Implementation procedures and duration	Expected outcome	Implementation agency	Criterion
Conduct survey on forming units in National Police Agency and Central Intelligence Agency and achieve the goal (2010-2012)	Cybercrime investigation, inquiry and court investigation improve	Central Intelligence Agency and National Police Agency	Number of cybercrimes tried at court
Develop national capacity to fight against cybercrimes, collect evidence of the crime, execute investigation in the crime scene and make forensic analysis on computer crimes, provide responsible agencies with required hardware/ software, and improve the operation of human resources (2010-2015)	Operational capacity of the police and judicial agencies has improved	CIA and NPA	Number of the cybercrimes investigated
Develop and publish training manual on how to conduct cybercrime investigation and cybercrime scene investigation; enroll inspectors and forensic officers in trainings; and develop awareness regarding prevention and investigation of cybercrimes (2010-2015)	Skill and knowledge of law enforcement officers and judicial employees improve	ITPATA, NPA and CIA	Number of the trainees

In Mongolia, there were two cybercrime cases were tried in 2015. To be more specific, on 2015.03.12 at the primary court trial#314 of district a citizen E. Sh was found guilty of intentional invention, use and dissemination of virus program but according to the article 72.1.1, criminal code, the case was dismissed because period of investigation was expired. Also on 2015.03.12 at the primary court trial#317[30] of district citizens E. M and N. B were found guilty, according to article 229.1, special part of the criminal code, of invention, use and dissemination of a program capable of performing deletion, shut off, alteration and copy of computer data without authorization. And again both suspects' cases were dismissed (N. B under the article 135.2 and E.M under the article 135.1). E. M was actually convicted of violation of mail communication privacy of four citizens. However, on the basis that investigation period had been expired, suspect was released without any charges.

So here it is seen clearly seen that there have not been many cases related to cybercrimes tried at court in Mongolia. In addition the cases that were tried all belong to the same category of 9 categories of cybercrimes. Also the fact that suspects were accused of committing offences stated in the chapter 25 along with offences other than those in the chapter 25 at the same time might had been caused because of the lack of complex legal regulation on socially harmful cybercrime. As for the offenders they were unemployed suspects with no high-education who had not been convicted of any offences previously. Therefore it can be concluded that the tools and methods used to commit cybercrime are easily accessible and control on any media content that shows and encourages cybercrime is very weak.

And because offenders of cybercrime are non-professional amateurs, it is required to improve the activity to raise awareness of cybercrime among those who face the risk of committing the crime most. Among the offenders, there were many minors who did not fully realize that they were committing crime and what the consequences of their action would be.

It will be too hasty and wrong conclusion to say that, in Mongolia, rate of cybercrime committed is very low and the crime itself is not very serious offence that threatens national security. But the crime rate seems very low

[30] L.Galbaatar. Resolving a cybercrime case by a court (Training handbook for judges, prosecutors and investigators). NUM Press Publishing. Ulaanbaatar. 2015. p. 62

only because many of the cybercrime victims do not report it to the police for reasons like business confidentiality. In this regard, Ch. Erdenebat, an associate professor of the School of Computer Science and Management, Mongolian University of Science and Technology said "... there was a nationwide network failure occurred at the Commercial Bank, the one with most branches in Mongolia. All branch offices including ones were not able to function. Commercial Bank's ATMs were out of service too. The network or system failure occurred around 9.20 a.m. So the bank worked until 9 p.m for extra work hours. In the years of 2007 and 2008, websites of 66 state organizations and institutions, 40 public offices, 64 educational facilities, 6 bank offices, 64 companies, 10 media/press organizations and 80 other subjects were cyberattacked by hackers" in his speech "Research on Websites of Mongolian Banks: SSL, WAF, metadata" delivered on 2012.12.14.

3.4. Legal Regulation on Data[31] Protection

Individual's data is daily collected at the various institutions of state organization, banking, transportation, mobile operator, hospital, education and shopping whenever he/she is provided service. At present, there is a high risk of losing individual's or institution's privacy uncertainty of legal regulation and legal education of citizens.

Under the order#15 issued on 2014.01.14 by the head of Information Technology, Post and Telecommunication Authority, a team to develop draft law of "Data Protection" was formed. The team members consisted of experts from the Information Technology, Post and Telecommunication Authority; Cyber Security Department; Communications Regulatory Commission; National Data Center; National IT Park; Mongolian University of Science and Technology; and Mongol Bank[32]. When the draft is passed and adopted as a law, processes like creation, collection, storage, protection, usage, possession, development, authorization, deletion, control, dissemination and evaluation of data will be legally regulated. Project implementation unit (formed under the order#09 issued on 2014.08.14 by the secretary general of the National Security Council) of "Developing National Security Policy

[31] Data - a set of values of qualitative or quantitative variables; restated, pieces of data are individual pieces of information

[32] Towards Open Data Development in Mongolia by Amarsanaa Ganbold, Tsolmon Zundui. 2014.11 http://www.slideshare.net/amarsanaag1/towards-open-data-development-in-mongolia

and Relevant Legal Documents" was introduced with the draft and, the unit and the team are working in cooperation now[33].

3.5. Legal Regulation on Censorship

According to the clause 6.2.1, "General Provisions of Regulation on Digital Content"[34] (amended by the resolution#18, 2012 and resolution#40, 2014), a supplement to the resolution#8 by the Communications Regulatory Commission, if any website provided by the website hosting service providers has users' comment section, the site is required to have word filter program issued by the regulatory commission.

However, it is still uncertain who created the vocabulary of the word filter program for there is no linguistics scholars participated. Even more there is no official statement/approval made regarding this program. Therefore suspicion arises that words included in the word filter program vocabulary can be added or deleted by the demand of political parties or in relation to the political phenomenon (like elections etc). And in the General Provision there is a clause 6.2.4 saying that "IP Address of the user must be shown in full above his/her comment on display". This clause definitely violates one's right to privacy. To avoid tracking one's IP address and respect one's right to privacy, users are given right to conceal their names. And journalist's right to conceal his/her information source might be violated by the clause 6.2.4, too[35].

The clause 3.5 says: "According to the article 12.3, Communications Law, host/owner of the news and information website running in Mongolia must be registered at the Communications regulatory Commission". There are 106 websites registered at the CRC running in Mongolia, so far[36].

As said in the clause 4, the General Provisions of Regulation on Digital Content, process of development, dissemination and advertising should be in compliance with the National Security Concept (particularly, articles 3.3.3 - Strengthening National Unity and 3.3.4 - Social Stability), and

[33] World Bank. Mongolia-Diagnostic Review of Consumer Protection and Financial Literacy Volume II - Comparison with Good Practices. 2012. p.35 https://www.mongolbank.mn/documents/financialliteracy/wsurvey2.pdf

[34] Communications Regulatory Commission. "General Provisions of Regulation on Digital Content" http://crc.gov.mn/file/newfile/togtool-2014-40.pdf

[35] "Freedom Situation of e-Media" a speech given at "Online Freedom" conference by J. Jargalsaikhan, head of the e-information center, 2015.03.30

[36] Websites and blogs registered online at the Happywebs.mn http://happywebs.mn/more.php?id=15

development and dissemination of contents that contradict with provisions of following laws and regulations are considered illegal: Law Against Prostitution; Law on Human Trafficking; Crime Prevention Law; Criminal Code; Law on Control of Narcotics Drugs and Psychotropic Substances; Law on Advertising Regulation; Law on Copyright and Relevant Rights; Law Against Drinking; Law on Children's Right; Parliamentary Electoral Law; and article 3.6.1.2, National Security Concept (restrict outside entities' attempts to influence the social psychology, social stability and individual consciousness and ethics of Mongolians).

The CRC has announced that, by March 30, 2015, 214 websites have been denied of access from Mongolia by the decision of state inspector of the State Agency for Intellectual Property and other relevant agencies for violating Law on Copyright and Relevant Rights; Law Against Prostitution; Law on Children's Right; Law on Advertising Regulations; Criminal Code; Competition Law; Law on Protection of Consumer's Right; requirement of the CRC; and international treaties and conventions Mongolia is member of. The CRC has also declared that access to these websites in Mongolia would be restored if they fix their breaches completely and state inspector from the relevant agencies approves their correction as satisfactory[37].

CONCLUSION

Core of the data security is cyber security. How to ensure the cyber security is reflected quite clearly in the relevant laws of Mongolia and national security concept. However, cyber security is growing even more dependent on international multilateral cooperation. In such situation it has become mandatory for Mongolia to join the international cooperation. And core and legal scripture of the cooperation is the Budapest Convention on Cybercrime.

Since 2010 Mongolia has taken more and more active measures, domestically as well as internationally, to protect human rights and freedom in online world. We have learnt from international experiences of exchanging information and methods to work safely online. But the fast grow of Mongolian e-governance alone can not be considered as proof of ensured protection of human rights and freedom online.

[37] Domains with violation. Communications regulatory Commission 2015.03.30, http://www.black-list.mn/index.php

The need to adopt specially designed laws (law to ensure cyber security, law on data protection etc.) is growing even stronger because differences between capacity and skills possessed by the state organizations and civil servants responsible to protect human rights and freedom are not very high.

But the crime rate seems very low only because many of the cybercrime victims do not report it to the police for reasons like business confidentiality. And again the number of cybercrime cases tried at the court is too few because the victims are unaware of the crime or do not report it to the police to keep their business confidentiality intact. Free online expression of opinion in the forms of leaving comment, producing content and disseminating it is regulated by the procedures of state agencies but not by court decision. Although Mongolian government recognizes the importance, at the policy level, of international cooperation in addition to developing national laws and procedures to protect citizen's online rights and freedom, practical achievement regarding cooperation is still very weak.

To say lastly, even when Mongolia is ready to join the Budapest Convention on Cybercrime, preparatory works to join the convention has been set and done yet.

BIBLIOGRAPHY

Laws:

1. Constitution of Mongolia, 1992
2. Convention on Cybercrime, 2001
3. Criminal Code of Mongolia (ammended), 2002
4. Criminal Procedure Law of Mongolia, 2002
5. Criminal Code of Mongolia (revised), 2016
6. National Security Concept of Mongolia, 2010
7. Supplement#2 - "Implementation plan of the national programme for information security", the Government Resolution#141 passed in 2010
8. Communications regulatory commision of Mongolia: "Terms and requirments of regulating digital contents" 2011

Reports, news and statistics:

1. Chart of signatures and ratifications of Convention on Cybercrime. Status as of 01/04/2016
2. Statistics. Cyber Security Department, General Intelligence Agency of Mongolia. 2016.02
3. International Legal Documents of Mongolia. Ministry of Foreign Affairs Mongolia
4. World Bank. Mongolia-Diagnostic Review of Consumer Protection and Financial Literacy Volume II - Comparison with Good Practices
5. Websites and blogs registered online with the Happywebs.mn
6. Domains with violation. Communications regulatory Commission 2015.03.30
7. 5th APT Cybersecurity Forum (CSF-5)
8. Reflections on the 5th Freedom Online Conference in Mongolia, 2015.05
9. MNCERT/CC - Mongolian Cyber Emergency Response Team/ Coordination Center

Articles and speeches:

1. Judicial General Council of Mongolia. Training manual for criminal law. p 115, Ulaanbaatar, 2015
2. Explanatory Report. Convention on cybercrime.
3. Transnational organized crime: the globalized illegal economy. UN Office on Drugs and Crime
4. Towards Open Data Development in Mongolia by Amarsanaa Ganbold, Tsolmon Zundui. 2014.11
5. Ж.Жаргалсайхан /МСНЭ-ийн Цахим мэдээллийн мэргэжлийн төвийн дарга/. Цахим хэвлэл мэдээллийн хэрэгслийн эрх чөлөөний төлөв, байдал /илтгэл/ 2015.03.30, "Онлайн эрх чөлөө" хэлэлцүүлэг. МТУП-ийн хурлын танхим. "Freedom Situation of e-Media" a speech given at the "Online Freedom" conference by J. Jargalsaikhan, head of the e-information center, 2015.03.30
6. L.Galbaatar. Resolving a cybercrime case by a court (Training handbook for judges, prosecutors and investigators). NUM Press Publishing. Ulaanbaatar. 2015.