World Vision

ISSN: 2078-8460

Vol. 12 • No. 1 • June 2018

A Study on Information and Communication Technology Act for Cyber Security

Dr. Kallol Kumar Moulic*

Abstract

This is the era of Information and Communication Technology (ICT). Bangladesh is trying to become modern in case of ICT. Present government is trying to make Bangladesh as a digital country in every sphere of country and Government is successful. But some criminals are doing different crimes by using the ICT. To prevent crimes, present government has made an act. A study was undertaken to know about the Information and Communication Technology Act 2006 and identify the reasons of amending concerned items of ICT Act 2006, to assess the integral linkage gaps of the amendments of ICT Act 2006 and to determine the discipline wise coverage of the ICT Act by laws. The study was survey and case study type. The study was conducted 7 divisions of Bangladesh. Purposive sampling method will be used for the study. Total 175 respondents were selected for the study. Data were collected from primary and secondary sources. Primary data were collected from the respondents of the study area. Secondary data were collected from books, journal, research report, internet etc. Questionnaire was used for data collection. Data were collected by face to face interview with the respondents. Collected data were tabulated and analyzed by using computer program Microsoft Excel. From the study it was found that maximum common people are not aware about the ICT act. The people who knew about the act have opined to correct the act. The result revealed that some people blackmailing other people, harassing different ways, enjoying illegal facilities by threat, abolishing opposite concepts. Police do not have the required ICT skill, ICT skilled man do not have legal knowledge, Implementers have very few ideas about application fields, the laws and by laws are not clear for effective decision, punishment sector is made opaque by civil administration. From the study it was found that some legal experts opined that the changed section is of extreme action, ICT act has contradiction with the constitution of Bangladesh, is non bailable and financial punishment is very high, need regular amendment and per country's available ICT Lab facilities and there should have bail provision. Publicity should be done for ICT Act. ICT skilled persons should be developed. ICT Laboratories/Studios should be established. One or more cyber appellate tribunal should be established. Workforce of professionals skilled in cyber security should be created a through capacity building, educational programs and training.

Keywords: *Information and Communication Technology, ICT Act, Cyber Crime, Cyber Security, Misuse, Problems.*

* Advocate, Supreme Court of Bangladesh.

1. Introduction

At present Bangladesh developing country and trying best to be a developed one. In order to digitalize Bangladesh there is no alternative to secured technological advancement among which tenable internet using should prevail in priority. This advancement demands ICT experts of which we have great lacking. With the advent of technology human beings are becoming exclusively dependant on automation and we can see its influence on all spheres of our life. The history of automation began when Babbage invented computer and especially a new horizon was opened before us with the invention of network particularly the Internet and World Wide Web (WWW). Internet has become the backbone of all kinds of communication systems and it is also one of the most important sources of knowledge in the present digitalized world. It is a *network of networks* that consists of billions of private and public, academic, business and government networks of local to global scope that are linked by copper wires, fiber-optic cables, wireless connections, and other technologies. The World Wide Web is a huge set of interlinked documents, images and other resources, linked by hyperlinks and URLs. The internet allows computer users to connect to other computers and to store information easily across the world. They may offer to do this with or without the use of security, authentication and encryption technologies, depending on the requirements. This free access to network creates privileges to some highly skilled criminals to do illegal deeds in the cyber world. The most common evil doings are crashing a computer system, theft of information contained in electronic form; e-mail bombing, data diddling, financial fraud like unlawful transfer of money by breaking the security code of credit cards, denial of services and virus attack. But the prevention and remedy for these offences through the structural and legal framework are inadequate in our country.

By considering the aforesaid incidences present government of the People's Republic of Bangladesh has passed an act Information and Communication Technology Act 2006 Act undertaken by the Parliament received approval from the President on 23 Ashwin, 1413 corresponding to 8 October 2006. On 6 October 2013, the Bangladeshi Parliament amended the Information and Communication Technology (ICT) Act, 2006. The amendments made many offences under the Act non-bailable1 and cognizable. 2 The amendments also imposed a minimum prison sentence of seven years for offences under the Act and increased the maximum penalty for offences under the law from ten to 14 years' imprisonment. The stated objective of the ICT Act is 'the legal recognition and security of information and communication technology.' However, the amendments to the Act appear designed to stifle the legitimate exercise of public criticism and to subject various persons including journalists, bloggers, and human rights defenders to arbitrary detention.

2. Objectives of the Study

The objectives of the study are as follows:

1. To know about the Information and Communication Technology Act 2006 and identify the reasons of amending concerned items of Information and Communication Technology Act 2006.
2. To assess the integral linkage gaps of the amendments of Information and Communication Technology Act 2006.

3. To determine the discipline wise coverage of the Information and Communication Technology Act by laws.

3. Methodology of the Study

3.1 Study design: The study was survey and case study type.

3.2 Study area: The study was conducted 7 divisions of Bangladesh.

3.3 Sampling method: Purposive sampling method will be used for the study.

3.4 Sample size: Total 175 respondents were selected for the study.

3.5 Sources of data: Data were collected from primary and secondary sources.

3.6 Sources of primary data: Primary data were collected from the respondents of the study area**.**

3.7 Sources of secondary data: Secondary data were collected from books, journal, research report, internet etc.

3.8 Tolls for data collection: Questionnaire was used for data collection.

3.9 Method of data collection: Data were collected by face to face interview with the respondents.

3.10Analysis of data: Collected data were tabulated and analyzed by using computer program Microsoft Excel.

4. Variable

Total respondents =175 (One hundred seventy five) persons

A. Respondents

1. Policing Professionals
2. Computer Technologists/Programmers
3. Satellite cable owners
4. Respective functional professionals

B. Site and minimum coverage

1. Dhaka City Corporation 50% area
2. Divisional City-20%
3. District-20%
4. Sub-district-10%

C. Professional Seniority

1. Policy level
2. Executive level
3. Operational level
4. Student level

5. Results and Discussion

Table 1: Age of the Respondent

Age (in Year)	Frequency	Percent	Cumulative Percent
21-30	32	18.29	18.29
31-40	44	25.14	43.43
41-50	42	24	67.43
51-60	39	22.29	89.72
61 and Above	18	10.28	100
Total	175	100	

Source: Field Survey, 2017

Age of the Respondent has shown in the above table. From the result it was found that age group 31-40 years was 25.14% which was the maximum and age group 61 years and above was the minimum. Age group 41-50 years was 24%, age group 51-60 years was 22.29% and age group 21-30 years was 18.29% respectively.

Table 2: Gender of the Respondent

Gender	Frequency	Percent	Cumulative Percent
Male	153	87.4	87.4
Female	22	12.6	100.0
Total	175	100.0	

Source: Field Survey, 2017

Gender of the Respondent has shown in the above table. From the result it was found that male respondents were 87.40% which was the maximum and female respondents was 12.60% which was the minimum.

Table 3: Profession of the Respondent

Profession	Frequency	Percent	Cumulative Percent
Private Service	18	10.3	10.3
Govt. Service	6	3.4	13.7
Business	61	34.9	48.6
Advocate	64	36.6	85.2
Student	26	14.8	100.0

Profession	Frequency	Percent	Cumulative Percent
Private Service	18	10.3	10.3
Govt. Service	6	3.4	13.7
Business	61	34.9	48.6
Advocate	64	36.6	85.2
Student	26	14.8	100.0
Total	175	100.0	

Source: Field Survey, 2017

Profession of the Respondent has shown in the above table. From the result it was found that 36.60% respondents were advocate which was the maximum. Because it was a law related research, so; maximum involvement should be advocate. Government service holder was 3.40% which was the minimum. On the other hand, 34.90% respondents were businessmen, 14.80% respondents were study and 10.30% respondents were private service holder.

Table 4: Educational Qualification of the Respondent

Educational Qualification	Frequency	Percent	Cumulative Percent
BSS	29	16.56	16.56
MSS	6	3.42	19.98
CSE	17	9.71	29.69
B. Sc.	11	6.28	35.97
MSC	12	6.86	42.83
LLB	64	36.6	79.43
Diploma Engineer	7	4	83.43
MBA	16	9.14	92.57
M. Com	13	7.43	100.0
Total	175	100.0	

Source: Field Survey, 2017

Educational Qualification of the Respondent has shown in the above table. From the result it was found that. Maximum 36.60% respondents were LLB Degree holder i. e. advocate which was the maximum. Because it was a law related research, so; maximum involvement should be advocate. 3.40% respondents were MSS degree holder which was the minimum. ON the other hand 16.56% respondents were BSS degree holder, 9.71% respondents were CSE

degree holder, 9.41% respondents were MBA degree holder, 7.43% respondents were M. Com degree holder, 6.86% respondents were M. SC. Degree holder, 6.28% respondents were B. Sc. Degree holder, 4% respondents were Diploma Engineer.

Table 5: ICT Gap within Department

ICT Gap within Department	Frequency	Percent	Cumulative Percent
Police do not have the required ICT skill	24	13.7	13.7
ICT skilled man do not have legal knowledge	52	29.7	43.4
Implementers have no idea about application fields	20	11.4	54.9
The laws and by laws are not clear for effective decision	64	36.6	91.4
Punishment sector is made opaque by civil administration	15	8.6	100.0
Total	175	100.0	

Source: Field Survey, 2017

ICT Gap within Department has shown in the above table. From the result it was found that 36.6% respondents replied that the laws and by laws are not clear for effective decision which was the maximum and 8.6% respondents replied that punishment sector is made opaque by civil administration which was the minimum.

Table 6: Respondents Knowledge on ICT Act

Whether Respondents have Knowledge on ICT Act	Frequency	Percent	Cumulative Percent
Yes	46	26.3	26.3
No	129	73.7	100.0
Total	175	100.0	

Source: Field Survey, 2017

Respondents Knowledge on ICT Act has shown in the above table. From the result it was found that 73.70 Respondents have no Knowledge on ICT Act which was the maximum on the other hand 26.30% respondents have Knowledge on ICT Act which was the minimum.

Table 7: If Yes, Respondents' opinion on correction of ICT Act

Respondents' Opinion	Frequency	Percent	Cumulative Percent
Strongly agreed in total law	22	47.83	47.83
Agreed normally for some clauses	16	34.78	82.61
Partially agreed for some clauses	8	17.39	100.0
Total	46	100.0	

Source: Field Survey, 2017

Respondents' opinion on correction of ICT Act has shown in the above table. From the result it was found that 47.83% respondents were strongly agreed for changing the total law which was the maximum and 17.39% respondents were partially agreed for correction some clauses which was the minimum. On the other hand 34.78% respondents were agreed normally for correction of some clauses.

Table 8: Misuse of Present ICT Act in Bangladesh

Categories of misuse	Frequency	Percent	Cumulative Percent
Blackmailing people	65	37.1	37.1
Harassing community	75	42.9	80.0
Enjoying illegal facilities by threat	17	9.7	89.7
Abolishing opposite concepts	18	10.3	100.0
Total	175	100.0	

Source: Field Survey, 2017

Misuse of Present ICT Act in Asia has shown in the above table. From the result it was found that 42.90 % respondents replied that ICT Act is using for harassing community which was the maximum and 9.70% respondents replied that ICT Act is using for enjoying illegal facilities by threat which was the minimum. On the other hand 37.10% respondents replied that ICT Act is using for blackmailing people which was very alarming percentage and 10.30% respondents replied that ICT Act is using for abolishing opposite concepts.

Table 9: Respondents' opinion about efficiency of Law enforcing agencies

Respondents' opinion	Frequency	Percent	Cumulative Percent
Strongly Agreed	15	8.6	8.6
Agreed	28	16.0	24.6
Partially agreed	132	75.4	100.0
Total	175	100.0	

Source: Field Survey, 2017

Respondents' opinion about efficiency of Law enforcing agencies has shown in the above table. From the result it was found that 75.40% respondents were partially agreed that present law enforcing agencies has efficiency for implementing ICT Act which was the maximum and only 8.60% respondents were strongly agreed that present law enforcing agencies has efficiency for implementing ICT Act which was the minimum and only 16% respondents were agreed that present law enforcing agencies has efficiency for implementing ICT Act.

Table 10: Problem of ICT Act

Problem of ICT Act	Frequency	Percent	Cumulative Percent
The changed section is of extreme action	62	35.4	35.4
It has contradiction with the constitution of Bangladesh	29	16.6	52.0
It is non bailable	24	13.7	65.7
Financial Punishment is very high	49	28.0	93.7
Others	11	6.3	100.0
Total	175	100.0	

Source: Field Survey, 2017

Problem of ICT Act has shown in the above table. From the result it was found that 35.4% respondents replied that Problem of ICT Act is the changed section is of extreme action which was the maximum and 6.3% respondents replied that

Table 11: Suggestion for improvement of ICT Act in Bangladesh

Suggestion	Frequency	Percent	Cumulative Percent
Need regular amendment and per country's available ICT Lab facilities	164	93.7	93.7
There should have bail provision	11	6.3	100.0
Total	175	100.0	

Source: Field Survey, 2017

Suggestion for improvement of ICT Act in Bangladesh has shown in the above table. From the result it was found that 93.7% respondents replied that regular amendment of ICT Act in Bangladesh is necessary and per country's available ICT Lab facilities which were the maximum and 6.3% respondents replied that there should have bail provision in ICT Act which was the minimum.

6. Conclusion

At present we are a developing country and trying to become a developed one. In order to digitalize Bangladesh there is no alternative to secured technological advancement among which tenable internet users should prevail in priority. This advancement demands ICT experts of which we have great lacking. The state should move forward for creating such experts with indispensable national ventures. Besides this, statutory shields should be made most effective by executing the aforesaid course of actions. Finally, we have to remember that technology is such a thing which is changing its nature and direction every moment and we have to achieve the maximum capability to accommodate its change in every moment change both in physical and virtual world for a perpetual existence.

In my research I found Cybercrime has already become a major concern in both private as well as public sector in Bangladesh. During the last decade private and public sectors have done a revolution with the use of technical enhancement. Due to unauthorized intervention to the system, company loses huge confidential information which caused a large amount of financial loss. It has already been identified that especially Financial Institutions are the most threatened organization for cybercrime that at the same time reflects to the personal life. Some development partners have started working how to tackle cybercrime and improve effective communications and stop cyber crime in their institutions. In my concern as the use of computers has grown, cybercrime has become more important. Cybercrime, as a transnational crime, is a global issue with a global impact. Increased sophistication of cybercrime attacks and vulnerability of information available online is serious concern for institutions, law enforcement agencies and other stakeholders.

In my research journey I would sincerely try to find the present level of the implementation of cyber laws in Bangladesh and also try to find suitable models for enforcement of cyber laws, prevention of cyber crimes and training requirement of enforcement authorities - through my research which would be of help for government and all other stake holders in the process and especially to the benefit of the society in creating fearless environment where they will have happy surfing, e-banking, e-shopping and e-mailing internet experiences for their lifetime.

The presence of cyber crimes relies heavily on the Internet and online activity, and as a result, regulations and oversight of this type of activity has been expressed in the spectrum of Cyber Law. Cyber Law is a fairly expensive legal field that consists of a variety of avenues and jurisdictions, including the ethical and moral use of the Internet for lawful and legal purposes.

Basically, there are some notable cyber crimes have been committed in Bangladesh. The gradual dependence and extensive use of computer and information technology by the financial institutions like bank, insurance company, and other non-government organizations increase the fear of commission of cyber crime here. Computer has been used as a tool of crime like making forged certificates and documents for a number of years in Bangladesh though the incident of targeting computer or computer system is very unusual. The use of information and communication technology has been playing a vital role in the 21st century due to globalization and the government is encouraged to adapt the coming future. The present government concepts of Digital Bangladesh is an Idea that includes the IT use for management, administration and governance to ensure transparency, accountability and answerability at all levels of society and state. But cyber crime is very important issue within the private and public sector in Bangladesh. Therefore the biggest challenge is that cybercrime in Bangladesh – A growing threat in digital marketplace.

7. Recommendations

The recommendations of the Study are as follows:

1. Publicity should be done for Information and Communication Technology Act

   Adequate education on the use of internet and internet basis Programmes is a must before start using the ICT apparatus. Government should create awareness among the uses about the possible Cyber crime through wide publication in the print and electronic media.

2. ICT skilled persons should be Developed

   To plug the holes of penetrating the cyber crimes adequate protection must be ensured by the concerned organization/authority.

3. ICT Laboratories/Studios should be Established

Government should create required facilities to build up trained ICT Personnel's having training all aspects of cyber crimes should be established in every districts and if possible up to Upazila level with objectives of maximum people aware and capable of using ICT knowledge.

4. Time to time amendment of ICT Act is necessary

   ICT is a dynamic subject and is continuously developing and changing. The nature of cyber crime is also changing to keep the stakeholders and supervisors and controllers constantly updated with the developments, time to time amendments in0 the law should be carried out and implemented.

5. Scammed should be avoided

   Always think before you click on a link or file of unknown origin. Don't feel pressured by any emails. Check the source of the message. When in doubt, verify the source. Never reply to emails that ask you to verify your information or confirm your user ID or password.

6. Right person should be called the for help

   Don't panic! If you are a victim, if you encounter illegal Internet content (e.g. child exploitation) or if you suspect a computer crime, identity theft or a commercial scam, report this to your local police. If you need help with maintenance or software installation on your computer, consult with your service provider or a certified computer technician.

7. Justice system should be established

   It is important issue that whatever the excellent rules was made by the government to stop the cyber crimes in their own country, one thing is very vital that justice system should be established properly within the experience manpower; otherwise the stakeholders will not be benefitted from the wonderful cyber crime rules. Remember the big role played by the law and enforcement agencies. Therefore, it requires very highly trained and qualified dedicated manpower to fulfill it s goal.

8. One or more cyber appellate tribunal should be established

   The Government should establish one or more cyber appellate tribunal. The appellate tribunal shall be constituted by one chairman and two members appointed by the government. To be appointed as a chairman of Cyber Appellate Tribunal, he must be either a former judge of the Supreme Court or existing judge of the Supreme Court or is eligible to be appointed as a judge of the Supreme Court. One of the two members of the tribunal shall be a retired District Judge or employed in the judicial service and the other member must be an experienced and skilled person in information and communication technology. They shall be appointed for 2-3 years. Cyber Appellate Tribunal shall have no original jurisdiction. It shall only hear and dispose of appeals from the order and judgment of the Cyber Tribunal and Sessions Court in appropriate cases. The decision of the appellate tribunal shall be final and it shall have the power to alter, amend, and annul the order and judgment of the cyber tribunal. The appellate

tribunal shall follow the appellate procedure of High Court Davison of the Supreme Court. Until cyber appellate tribunal is established, appeal may be heard by the High Court Division.

9. Pilot study should be developed for technical and logistics support for the cyber crimes team

   The Government should start pilot study to develop the technical and logistics support for the cyber crimes team and create better team within the work frame to tackle the total cyber crime network in national and international level. The pilot study should be conducted at the internet centers should reveal several issues on the internet scenario of internet users and help to frame the following main research objectives. The specific objectives of the pilot study be include: a)The nature and number of cyber crimes intimated to the cyber police in Bangladesh b)The nature and number of cyber cases investigated (and charge sheeted)by cyber police. c)The nature and number of cyber cases brought before the court and the effectiveness of the process of administration of justice in these courts.4.The nature and number of cyber criminals prosecuted by court and the nature and number of cyber cases left untried for technical defects and problems.5.whether the general public i.e internet users are aware of different types of cyber crimes and what is the level of their understanding and whether they are equipped to protect themselves from cyber crimes (while in internet use).6.whether the Bangladeshi's cyber police are properly trained to handle cyber crimes effectively. These are the factors should need to be considered in the pilot study in the cyber crime area to develop properly and work effectively.

10. Cyber secure system should be in defense Sector, generate adequate trust in ICT sphere, and enhance infrastructure capabilities for Bangladesh defense Sector;
11. A system should be set up to design all conceptual documents necessary for security implementation. The system will ensure documents to be in compliance with global security standards and best practice;
12. Information technology security should be established and enhance 24/7 incident response mechanisms to protect ICT infrastructure, rapid identification should be carried out of threats and risks, perform necessary responsive and preventive measures, in case of necessity crisis management should be provided through predictive, preventive, protective and recovery actions;
13. The protection and resilience of functioning of defense sector should be enhanced by operating 24/7 mechanisms applying best practice on establishment, acquisition, development and operation of information resources;
14. Research and analysis of emerging and unpredictable threats, risks and challenges on a regular basis should be conducted. Understanding of threats and assessment of their potential impact ensure enhancement of security arrangements. Preventive measures should be done in accordance with the research/analysis results for better combating rapidly changing threats.

15. Workforce of professionals skilled in cyber security should be created a through capacity building, educational programs and training;
16. Culture of cyber security and privacy confidentiality should be create for enabling users to act effectively in compliance with the defined rules;
17. Personnel should be encouraged to participate in cyber security related training and educational programs;
18. Close cooperation with national and international organizations should be established, facilitate the development of bilateral and multilateral relations;
19. Various guidelines should be developed by separate cyber security department that will immensely contribute to creation and enhancement of safe, effective and credible cyber security infrastructure in order to implement Cyber Security for Bangladesh".

References:

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. (2012). *Measuring the cost of cybercrime*.

Alam, S (2015), *Cybercrime and legal fabric of Bangladesh,* Bangladesh Law Digest-available athttp://www.bdlawdigest.org

Claessens, J., Dem, V., De Cock, D., Preneel, B., &Vandewalle, J. (2002). *On the security of today s online electronic banking systems.* Computers & Security, 213: 253-265

"Cyber-Crime in Bangladesh : A growing threat in digital market" available at :http://www.risingbd.com/english/cyber-crime-in Bangladesh- a - g rowing - threa t - in-di g i t a l -marketplace/28940

Douglas, T., & Loader, B. D. (2000). Cybercrime: *Security and surveillance in the information age,* Routledge

Florêncio, D., &Herley, C. (2010). Phishing and money mules. In Information Forensics and Security WIFS, *IEEE International Workshop* on pp. 1-5. IEEE

Federal Bureau of Investigation, Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit Washington, D.C. September 14, 2011

Global economic crime survey, (2016). *"How cyber-criminals targeted almost $1 bn in Bangladesh Bank Heist*",available at https://next.ft.com/content/39ec1e84-ec45-11e5-bb79-2303682345c8#axzz46NHKzCwH

Jaleshgari, R. (1999). *Document trading online.* Information Week, 755:

Moore.T, Clayton.R&Anderson.R (2009). "The Economics of Online Crime", *Journal of Economic Perspectives*, Volume 23, Issue no.3, Summer 2009, pp.3-20

Maruf,M.A, Islam, R, Ahmed, B(2010), Emerging Cyber Threats in Bangladesh: In Quest of Effective Legal Remedies, *The Northern University Journal of Law*, ISSN 2218- 2578,Volume I (2010)

Perumal, A.S., (2008) Impact of cyber crime on virtual Banking, *SSRN Electronic Journal* 10/2008

S. M. Nsouli and A. Schaechter, (2002). "Challenges of the e-banking revolution: Finance and development," *International Monetary Fund*, vol. 39, no. 3, pp. 231-254.

Shewangu D.(2015), Cyber-banking fraud risk mitigation- conceptual model, Banks and Bank Systems, Volume 10, Issue 2, 2015.

Siddique,I&Rehman S.(2011). Impact of Electronic crime in Indian Banking Sector - An Overview, *International Journal of Business Information Technology*, Vol-1 No. 2 September 2011

Vrancianu, M., &Popa, L. A. (2010). Considerations Regarding the Security and Protection of E Banking Services Consumers Interests. *The Amfiteatru Economic Journal*, pp- 1228: 388-403

Wall, D. 2001. 1 *Cybercrimes and the Internet*. Crime and the Internet.

Z. Liao and M. T. Cheung (2008), "Measuring customer satisfaction in internet banking; A core framework," *Communications of the ACM*, vol. 51, no. 4, pp. 47-51.
