

Seminar Paper

On

Cyber Security Strategies in Bangladesh: A Study on Social Media.

Submitted to

Dr. Muhammad Abu Yusuf
MDS

Bangladesh Public Administration Training Centre
Savar, Dhaka.

Submitted by

Md. Mongir Ahmed

Roll no. 124

Deputy Director (Deputy Secretary)
Department of Telecommunications
Post and Telecommunication Division

126th Advanced course on Administration and Development (ACAD)



Bangladesh Public Administration Training Centre (BPATC)

September 22, 2019

Cyber Security Strategies in Bangladesh: A Study on Social Media

ABSTRACT

In the age of globalization cyber security is the key element of international era. A National Cyber Security Strategy of a country reflects the state of that country's cyber strength which represents the aim and vision of the cyber security of a country. Social media has become the most popular and effective grounds for users. It also becomes a very popular media to practice unethical acts. This research paper describes and reveals the challenges of cyber securities and strategies to overcome that challenges. This study also focused on the acts in social media which are not ethical and lawful. The effects of these acts on the society and the way out from these environments are focused in this paper. The study uses qualitative method where questionnaires were given to respondents and also expert opinions were collected. So, the necessary steps should be taken to ensure cyber security and prevent unlawful and unethical activities on social media.

Key words: Cyber Security, Social Media, Unethical contents.

INTRODUCTION AND LITERATURE REVIEW

This is the age of globalization which makes the world easy by the very fast growing of internet technology. It plays an important role to achieve economic prosperity and credible defense of a country (Williams 2013). So, every state is in now under security threat. This security threats are also affecting our society. Worldwide every country is taken measure on this issue. This cyber security issue hampers the international peace and development. This scenario also effect in Bangladesh. There are so many strategies to ensure cyber security like Acts, Regulations, Guidelines, and Awareness and Technological solutions.

Social media is an unbelievable tool of communication. By using of social media now a day the communication became faster and easier. The society has benefitted in different ways by using social media. They can talk each other; find news, information, teaching materials, entertainment in a text form or in audio, image or in

video form. However, some people or users are doing unfair means through the evolution of social media and Technology. They are misleading and misusing the social media. They are using it negatively, uploaded unlawful, unethical and harmful contents in different social media. Some false information, fake news, disrespect to anybody, humiliate someone, objectionable image or video, distorted pictures, rumors, propaganda. In the view of freedom of speech, anybody can publish any statement in the social media if that content will not hurt anybody. The sufferers have not a significant way-out to do anything in Bangladesh on those contents which has been posted in different social media. There is a severe effect on their social and mental illness. This unethical posting of contents in social media is a serious offense which is unlawful and also harmful for society. A social awareness development is necessary for mass people and the users of social media. A measure like hide or remove of particular content should be taken immediate after posting of an unlawful content before goes viral of that content.

This study includes extensive research on Cyber Security Strategies in Bangladesh focused on social media emphasized on unlawful, unethical and harmful contents and about the measures to be taken on those contents. There are so many advantages with some disadvantages also. Unlawful, unethical and harmful contents of social media are increasing day by day. This study intends to know the views of users' and find out the measures to be taken for the betterment of whole society and also for the country. Also, Bangladesh government can use these results to take attention program, create regulations and necessary technological solutions on this major issue.

Various research contributions towards cyber security had been made formerly. A case study of review used qualitative comparison approach between 54 countries and the findings shows key reasons behind creating cyber security strategy. It implies the importance for creating cyber security strategy. The main drawback was, the conclusions they reached based on the study of existing National Cyber Security Strategy (NCSS) themes. Therefore the reliability of the themes could not be ensured (Sarkar. K 2019). Another Case study performed by the National Cyber Bureau of Israel on Cyber security policy model proposed a framework for the creation of cyber

security. The case study was a comparative research between the NCSS of countries that are considered world pioneers in technology (Deniel. B 2017). The study found some best practices that were followed by all the countries involved in the cross comparison of the study. However the limitation of the study is every country has some different agenda, therefore they certainly will have some differences while creating their strategies due to distinct national and international interests. The framework is flexible which can be considered as a positive aspect. However, Very insignificant attempts had been made formerly to evaluate the NCSS of Bangladesh in Context with the other countries.

Therefore this research is going to cover the research gap found in this context. As far as the national cyber security strategy of Bangladesh is concerned the strategy outlines a framework to manage risks of Bangladesh's cyber security which directly follows the GCA (Global Cyber Security Agenda of International Telecommunication Union). In line with this GCA, this strategy implies the prioritization of the strategic areas. These areas are – National Cybercrime legislation, reducing vulnerabilities in software products, raising awareness and International cooperation.

In order to secure the national cyberspace from internal and external threats, the Government of Bangladesh published The National Cyber Security Strategy of Bangladesh in March 2014. 'The Information & Communication Technology Act, 2006' known as ICT Act 2006 was initiated on 08 October 2006 (ICT Act 2006) is a legal framework of Bangladesh. Bangladesh Parliament amended this Act on 06 October 2013 (ICJ 2013) & Pornography control Act, 2012. Based on that criticism to ensure National Digital Security and Identification, Prevention, Suppression, Trial and other related matters, recently Bangladesh Parliament has accepted an Act which has been approved by the President of Bangladesh on 08 October 2018 named Act no. 46 of 2018 titled as "Digital Security Act 2018." 13 members National Security Council will be formed under section 12 of this Act. Prime Minister will be the Chairman of the council and a Digital Security Agency will be formed under section 5 of this Act. Director General (DG) will be the head of this agency. In chapter three of this Act assigns power to remove or block some data-information or contents by Bangladesh

Telecommunication Regulatory Commission (BTRC) subject to the request of Director General of said Agency (Digital security Act 2018). Besides this Law and Enforcing Security force can request BTRC to block or removal the contents via DG. If any contents published or propagated in digital media (Social media) which threaten the digital security that contents will be blocked or removed. Now a day BTRC is doing this by the help of International Internet Gateway (IIG) operators. A project titled "Cyber Threat Detection and Response" is going to implement by Department of Telecommunication (DOT) to ensure safe social media and safe internet for all. Very recent time, Digital Security Agency is formed but the activities of the agency yet to start. So, the proper functioning is not possible under this Act. In above context, there is some gap in strategies of ensuring Cyber Security and the blocking of harmful contents of social media. In this research that gap will be addressed.

PROBLEM STATEMENT

Cyber Security is an essential act for the security of a nation and up to for an individual. In a virtual world cyber threat can be come from inside the country and also from outside of a country. There are so many advantages of Social media with some disadvantages. By using social media now the life is so fast. At an instant anything can happen in social media. So, the strategy for cyber security is needed to ensure safe internet service. The versatility of social media platforms and the global reach of these platforms became people empowerment all over the world. Sometimes somebody uses this platform in a negative way. They create a lot of problems, including the use of social media to blackmail and defame of a community or a business or an individual. These might be competitors, dissatisfied customers or other people with an intention to grid. There are some studies on Cyber security in our country but there are not so specific studies on Social media contents. There are unlawful and unethical contents in social media which can harm the society and also an individual. Most of the social media broadly relies on self-governance. YouTube and Face book sites have their own rules and regulations. To remove any unwanted content they follow their own rules not our rules or norms and ethics. To overcome

this situation and to ensure cyber security the existing rules and guidelines should be updated and appropriate and the technological solutions should be developed for removing or filtering the unlawful, unethical and harmful contents from social media.

OBJECTIVES

The worldwide tremendous boom and easy accessibility of internet has created a pace in the exchange of information in the field of education, research, health, culture and other socio- economic sector. The evolution of social media has provided the aforementioned benefits by connecting people to the information super highway. On the other hand, the misuse of social media for promotion of unlawful and unethical contents like pornography and other harmful content delivery is leading youths, teens to generation. So, safe social media is needed for all. In this context, the objectives of this research work are as follows:

- i. To address the current cyber security policies in Bangladesh.
- ii. To identify the social media monitoring tool for reducing unethical contents in Social Media of the country.

RESEARCH QUESTIONS

- i. What is the current state of cyber security strategy available in Bangladesh?
- ii. What are the effects of unethical practices on social media and what measures are taken to control the unethical contents of social media?

RATIONALE OF THE STUDY

The whole world is now connected via internet which makes us virtually a global citizen. Cyber threat is not a national concern anymore rather a matter of global security. The importance of this research is important as it will define the current cyber security related policies and Acts in Bangladesh. To reduce the unlawful and unethical contents of social media proper legislations can be implemented properly.

This paper tries to identify the main strategy of cyber security in Bangladesh. There are no such type of research yet done for removing or filtering the unlawful and unethical contents from social media in Bangladesh. The findings of this research paper will contribute to filter the unlawful and unethical contents from social media. This paper will help to use safe internet service and also help to the Government to introduce measures for monitoring the social media effectively and efficiently.

CONCEPTUAL FRAMEWORK

Here we use conceptual framework for this research paper. The conceptual framework presents an integrated way of looking at a problem under study (Liehr & Smith 1999). It describes the relationship between the main concepts of this study. It is arranged in a logical structure to aid provide a picture or virtual display of how idea in a study relate to one another (Grant & Osanloo 2014). It shows a series of action to carryout in a research study (Dixon et al. 2001). This framework will make it easier to specify and define the concept within the problem of this study (Lase et al. 2012). It can be graphical or in a narrative form which will show the key variables. It is the simplest way to remedies the problem. It shows a series of activities the researcher intends to carry out in a research study (Dixon et al. 2001). The framework makes it easier for the researcher to easily specify and define the concepts within the problem of the study (Luse et al. 2012).

Cyber security consists of technologies, process and controls designed to protect systems, networks, programs, devices and data from cyber attracts, faction cyber security reduces the risk of cyber-attacks and protects against the unauthorized exploitation of systems, networks and technologies. Overall cyber securities are essential to given the conduits and manners of interacting with computer systems from suspicious behavior.

Government of Bangladesh has adapted a cyber-security declaration 2017 asking organization to develop actionable cyber security road maps to be approved and monitored by the top management.

The declaration said that the cyber organization would have to update their organizational chart identifying role and responsible for cyber security operations, entrusted with clear mandate, responsibilities and budget.

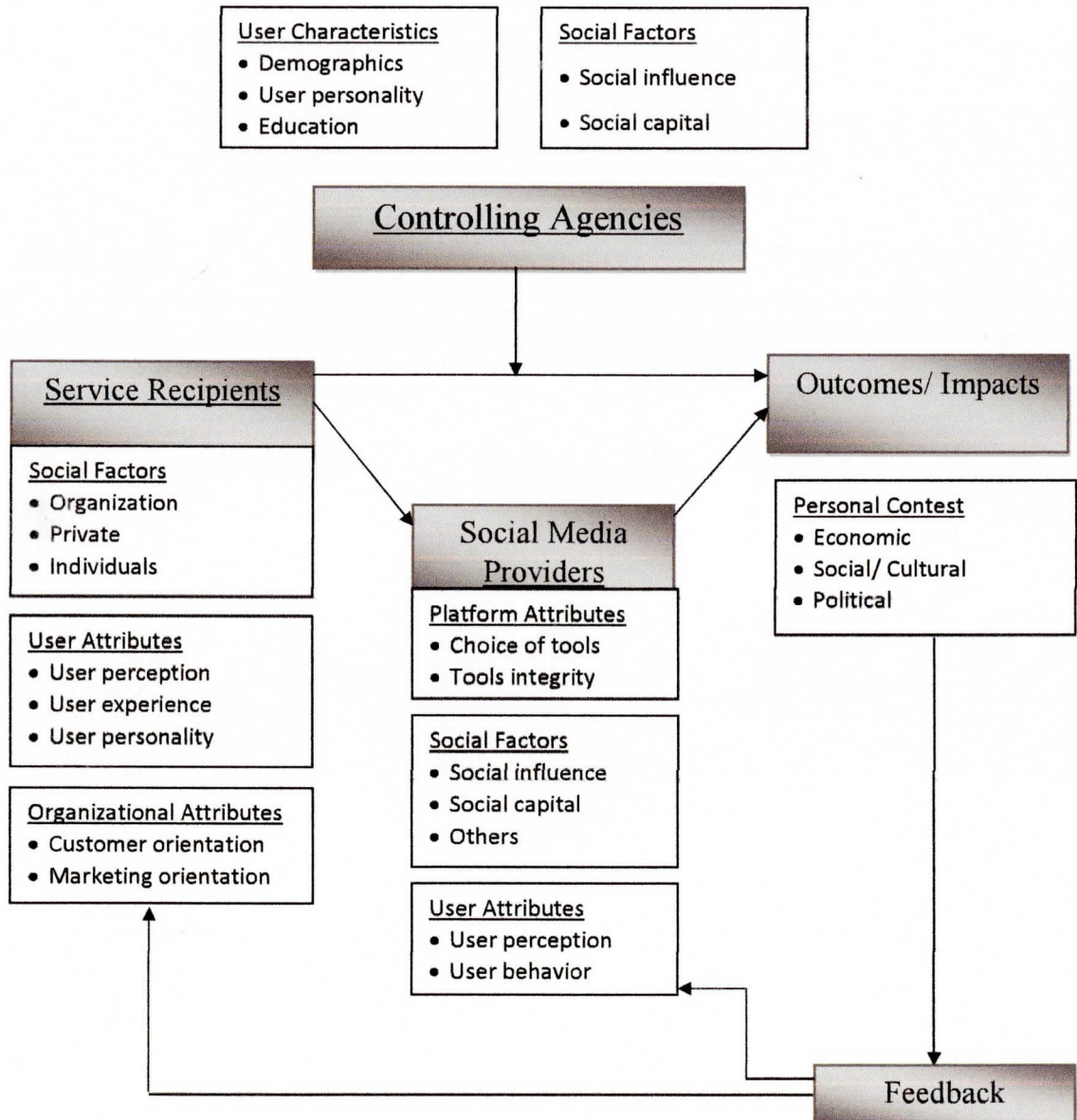
The declaration said that the nature and scope of cyber threats dictate that sustainable security of operations cannot be ensured by technology alone. It added that national organizations like Computer Emergency Response Team (CERT) can address only specific national threat and they are not expected to ensure operation at individual organization level. A study on cyber risk facing financial institutions conducted by the Bangladesh Institute of Bank Management (2017) shows that 28% of banks are 'totally unaware', 22% are 'unaware' and 20% has 'little idea' on cyber security.

It was the year before hackers stole \$101 million from Bangladesh Bank account with Federal Reserve Bank in New York, stirring global attention. Websites of various Government offices have suffered multiple cyber-attacks, including that of the BASIS and National Parliament also. A Computer Incident Response Team (CIRT) is formed by ICT Division and they identified 22 critical information infrastructures for monitoring of 24 hours, a team has formed including police, CID, detective branch and ICT division and providing training on it.

The proposed framework is divided into four main Parts. The parts are as follows:

- i. Controlling Agencies
- ii. Service Recipients
- iii. Social Media Providers and
- iv. Outcomes/Impacts

Each part of the framework has some characteristics, attributes and factors which will determine the behavior of social media.



Flow chart: Developed by author

METHODOLOGY

Research method is the methods which the researcher uses in conducting research operation. In either way, it refers to all techniques and procedures which research uses to collect information in his/her research study (Kothari 2004). This study mainly used qualitative research design. Qualitative research methods originated from social and behavioral sciences. Today our world is much more complicated and it is very difficult to understand what people think and what they perceive. Qualitative research method makes it easier to understand that as it is more communicative and also descriptive. So, the inferences can be drawn quite easily from the data that is obtained. Methods of qualitative research include observation and immersion, interviews, open-ended survey, focus groups, content analysis of visual and textual materials, and oral history. Qualitative researchers use their own eyes, ears, and intelligence to collect in-depth perceptions and descriptions of targeted populations, places and events. Their findings are collected through a variety of methods, and often, a researcher will use at least two or several above mentioned methods while conducting a qualitative study. This method is divided into two types, primary data and secondary data collection. The primary data are those data or information which is obtained directly from the study area. Usually primary data gathered through interview and participation. On the other hands, secondary data are collected through materials and document analysis of other works which have done by another researcher such as books, journals, websites etc. Qualitative research method is applied in this study in order to answer the research questions. This involves both primary and secondary data analysis. In this paper, interpretative documented analysis combined with content analysis is used. Moreover, 32 participants and four cyber security experts were selected as key informants for in-depth interviews. These interviews portrayed a better understanding of the way which cyber security strategy operates, intervenes, and effect and solutions to overcome unethical practices on social media with national security agendas. Interviews were taken in a semi structured procedure to give the interviewees an opportunity to elaborate on the subject matter. The 32 participants are from different districts/divisions of our country those who use social media but some of they lived in Dhaka and some are frequently move from home district to Dhaka city. The key

informants are key personnel of regulator- Bangladesh Telecommunications regulatory commission (BTRC), Chief Technical Officer and owner of Social media service provider that means International Internet Gateway and Project Director of ongoing government owned project related to cyber threat detection and response. Areas covered in the key informant interviews were how we can explain Bangladesh's cyber security strategy, how to reduce the unlawful and unethical contents on social media, how to improve the current policy in order to create a safe social media. Analysis of data was done based on both primary and secondary data for findings of this research.

DATA ANALYSIS AND RESULTS

The goal of this study was to address the existing cyber security policy and to identify the social media monitoring tool for reducing unethical contents of social media. Qualitative data were collected for this study. The collected data were analyzed by using logical and content analysis techniques. The analyses of collected data are summarized below:

1. State of Cyber Security Strategies available in Bangladesh

All of the key informants of this survey identified the following categories the cyber security strategies are working in Bangladesh. All of the key informants expresses their view in these regards are following:

Table-1: Cyber Security Strategies

Criteria	Present	Partially present/Absent
Research & Development		Partially present/Absent
Cyber security education		Partially present/Absent
Ongoing risk assessment		Partially present/Absent
Regulation and counter cyber-crime policy	Present	
Co-operation		Partially present/Absent

From Table-1, the detail analyses are as follows:

i. Research and Development

There are no national cyber security R & D activities in our country and still now priorities and necessary funds are not adequate to conduct research and development in this sector.

ii. Promote Cyber Security Education

Skill of Cyber security professionals in Administration, Managerial, Technical and Information assurance area is not enough to meet our security. It is necessary to increase the capacity and number of cyber security professionals and spreading the knowledge.

iii. Ongoing Risk Assessment

Information infrastructure is not resilience and tackling threats of cyber security are not enough. Strengthening of related infrastructure is very essential.

iv. Regulation and Counter Cybercrime Policy

The complexity of legal framework and logistic support are inadequate. Enhancement of law enforcement capabilities is very essential. Legal framework and all related Acts should be clearly defined about the activities and the consequences.

v. Co-operation

Conduct of training could minimize the gap of skill on cyber security and sharing of knowledge with the law enforcing agencies. Participation in international cooperation dialogue and coordination activities is very much important to take relevant steps to focus on mutual assistance.

2. Growth of internet subscriber of Bangladesh:

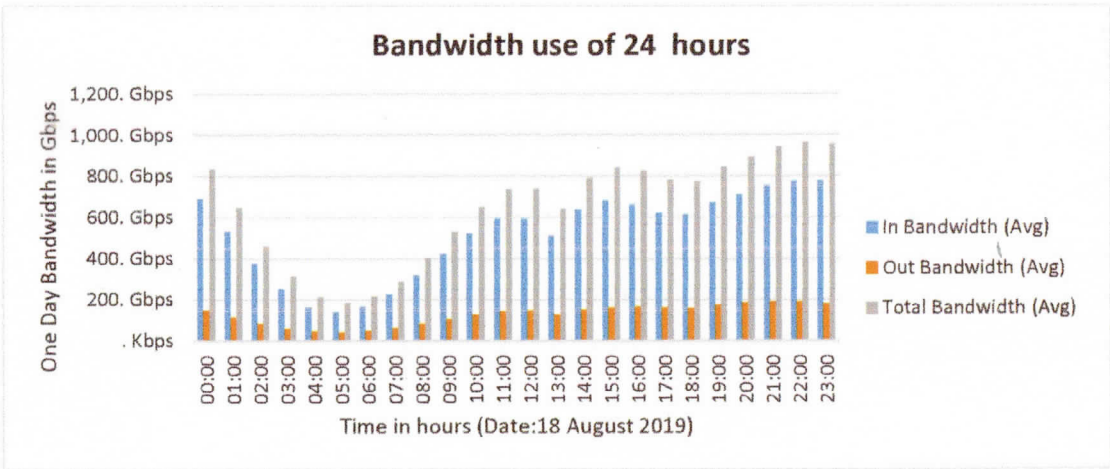
Table-2: Internet Users

Name of Month	Number of Internet Subscriber in Million
January'2019	91.421
February'2019	92.061
March'2019	93.102
April'2019	93.702
May'2019	94.445
June'2019	96.199

Source: Bangladesh Telecommunication Regulatory Commission (BTRC) (2019)

Internet subscriber means subscribers who have accessed the internet at least once in the preceding 90 days. The growth rates of internet users are varied from 0.64 to 1.86% in January '2019 to June '2019.

3. Bandwidth used in social media



Source: Department of Telecommunications (DOT) (2019)

Fig.1: Bandwidth used in social media

From figure-1, it is observed that in our country downloaded bandwidth is the maximum used bandwidth with respect to uploaded bandwidth. The total bandwidth used in social media is near about to 950 Gbps. At midnight highest bandwidth is used.

4. Most visited sites of social media

Table-3: Most visited social sites

Social Site	Number
Facebook	26
YouTube	21
Viber	11
Whatsapp	14
Others	7

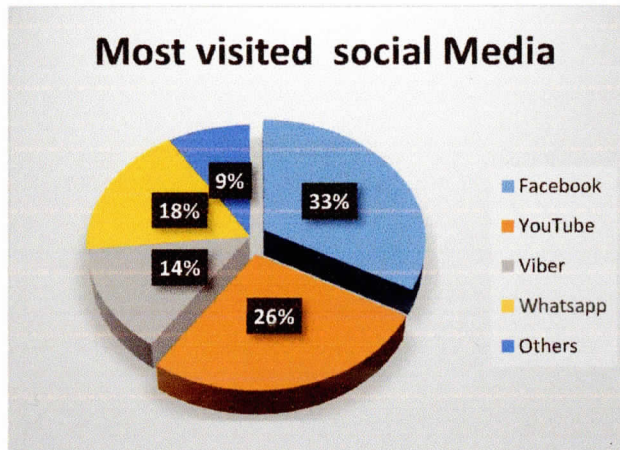


Figure-2: Most visited social media

The above figure-2 shows that Face book and YouTube are most visited sites.

5. Knowingness about rules, regulation to use social media

Table-4: Knowingness of respondents about rule and regulation

Yes	22
No	10

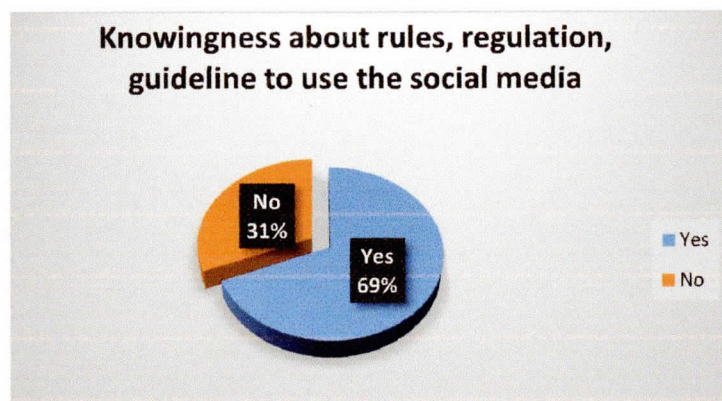


Figure 3: Knowingness about rules, regulation, guidelines to use the social media

31% of the participants do not know about rules, regulations and guidelines to use social media. So, the awareness development is needed.

6. Unlawful &Unethical practices on social media.

Table-5: Types of unethical practices

Fake account	Exposing of Govt. Services	Scams	Sharing of personal Problems	Showing exclusivity of one religion	Vulgar Language	Defamation or Humiliation
18	14	9	18	7	12	12

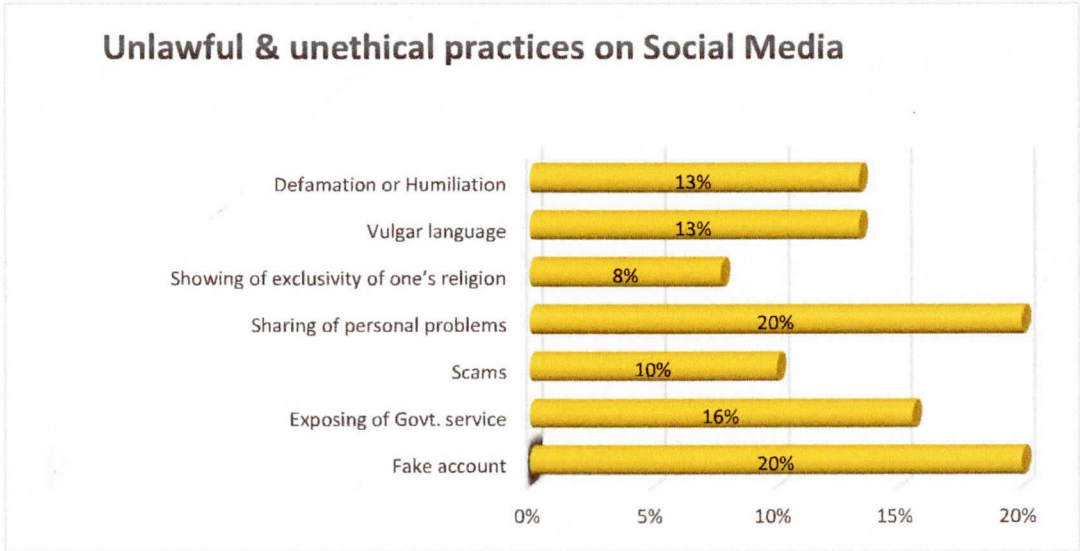


Fig.4: Types of unethical practices on social media.

Fig.4 shows that 20% of the respondents have seen sharing of personal problems and 20% fake accounts. Next the exposing of government services is 16% of the respondents. The third one by 13% are defamation or humiliation and vulgar language. Also, 10% & 8% are on scams and exclusivity of one’s religion.

7. Involvement in unethical acts.

Table-6: Involvement in unethical acts

Yes	1
No	31

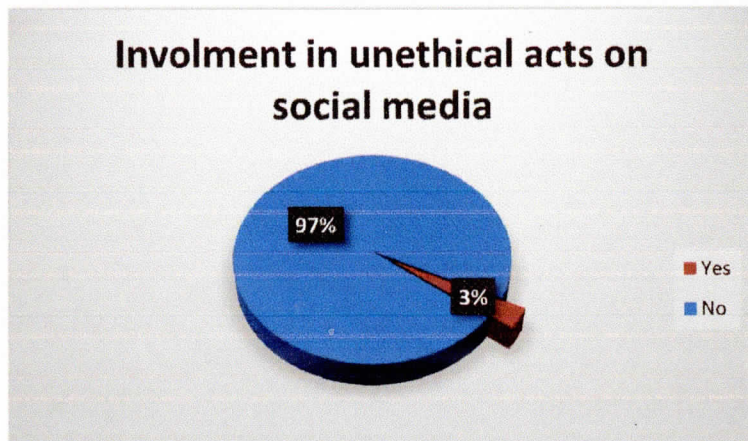


Fig.5: Participation in unethical acts.

Figure-5 shows 97% respondents are not involve in unethical acts on social media and 3% of the respondents have been involved in such practices.

8. Rumour against society or Government or Country should be continued in social media.

Table-8: Rumour

Yes	7
No	25

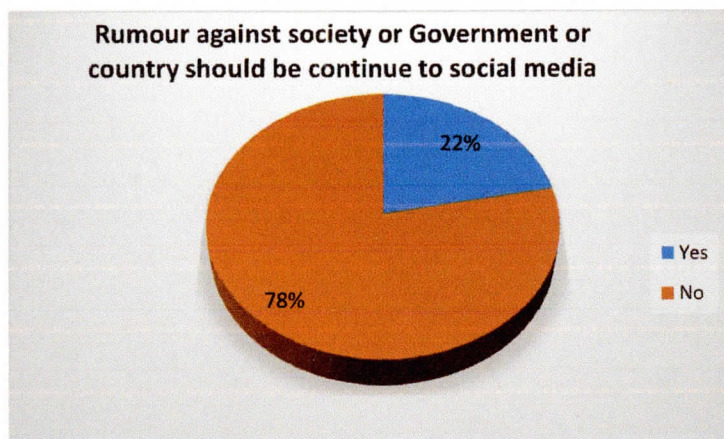


Fig.6: Continuation of Rumour against society or Country

In figure-7 there are 22% participants in favour of continue of rumour in social media. They think that there may some truth in that content. 78% respondents are agreed to take necessary measure against those rumour.

9. Measure against porn and betting sites &leakage of public Examination question paper in social media.

Table-9: Leakage of Question paper

Yes	24
No	8

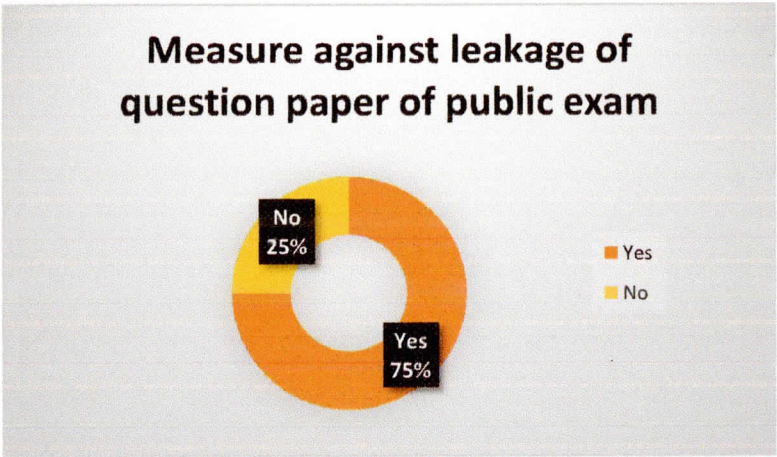


Fig.7: Measure against leakage of public examination question paper

All of the 32 respondents also stated that all unethical sites like pornography and betting should be blocked from social media. The Cyber Threat Detection and Response system which is installed by Department of Telecommunication (DOT) under Post and Telecommunication Division preliminary started their work. By this time, more than 20,000 porn sites and more than 2,500 betting sites were fully blocked by above mentioned system (DOT).

25% of the participants are not interested to take measure against leakage of public examination question paper and 75% are agreed to take measure against leakage of public examinations question paper.

10. Effect of unethical practices on social media.

Table-10: Effect of unethical practices

Name of effect	Number of respondents	% of Respondents
Depression	24	75%
Suicidal thoughts	17	53%
Stress	20	62%
Family reputation	18	56%
Disagreement	14	44%
Others	12	38%

From above table-10 it is mentioned that different types of effect on a person's well being. These are mainly Depression, Suicidal thoughts, Stress, Family reputation, Disagreement. Total respondents were 32. The impacts of all above factors are significant. Some of the respondents mentioned particular example of each type of effect. In others category effect like violent, seek revenge, drug addiction.

Effect of unethical and unlawful acts:

Discouragement or Depression

Depression of a person may occur in different forms. Very personal information or videos of anybody shared and becomes viral and different comments on it, then that particular person fall on depression. It may occur in discouragement, or in hopelessness or unhappiness of a person. Daily activities of a person are in physical activities, spending time with families, relatives and friends. If a person is not go within this activities and most of the time go through with social media, once upon a time he or she will be out of society. The bonding with family, friends or society of such person will decrease day by day and loneliness will occur to that person. In case of any problem that person will not be able to share his or her problem with other.

Suicidal Thoughts

Leading cause of a suicide is humiliation or defamation. This arises through negative criticism. Respondents mentioned that if the criticism continuously humiliates a person, once upon a time he or she thinks about suicide. They think that there are no way to solve the problem and suicide is the only way.

Stress

Mental pressure is the main cause of stress. Some respondents mentioned that if a person faces unethical acts on social platform against him, then mental pressure or stress developed in him. As a result, he or she gets sick and tends to illness. By creating fake account in social media some person circulate scams or defamation against anybody and results to get stress.

Family Reputation

Unethical practices on social media may disrupt family reputation of anybody. The forms of unethical acts are personal problem or information sharing, vulgar language. By the practices of above mentioned activities any individuals personal and family reputation will be damaged or disrupt.

Disagreement

The perception or thinking of individuals may differ. Any post by somebody in social media, create disagreement. Many people express their own perception or thinking. These perceptions are different from person to person. Unnecessarily social media became a ground of different opinion and also disagreement. If the post is unlawful, some person claims in favour of those contents. So, disagreement will occur in the society. In case of any religious issue, Government criticism, or vulgar issue result will be disagreement

Others

Sometimes somebody may outburst due to unethical practices against him. As a result that person might think about revenge against those who involved in that particular unethical practice.

12. Measures against unethical and unlawful practices

All of the respondents of this survey identified some tools to stop unethical and unlawful practices on social media. Those are summarized below:

- i. Role of Community
- ii. Role of Parents
- iii. Role of Government
- iv. Role of Schools
- v. Role of Religion Institutions
- vi. Role of Mass Media

Role of community

To create awareness on unethical practices or to reduce it society can arrange a get together and can invite a renowned person regularly. Most of the members of that society do not know about good or bad impact of such practices. So, through this type of discussion society can know about the consequences and to do the good things. Sharing of the problems each other and in line with our ethics community can take a vital role against unethical activities.

Role of parents

Relation between the Parents and their children's are most close in the world. At the time of grown up of children, parents and only parents can show and teach them about truth & false, good & bad, right & wrong. Parents are the first founder of children. Parents should spent time to their children. This time will be quality time. Parents should teach them about unethical behavior and the unlawful contents of social media. The monitoring is also needed from parents.

Role of government

To build a society and to build a nation the role of government is as a facilitator and as a controller. To protect the people of the society from unethical practices should form necessary laws and impose the laws impartially against those who are involved in such unlawful and unethical practices. Government should deploy technological system to filter the unethical contents before gets viral and able to block such platform.

Role of schools

The role of school is most significant way to teach ethics. Most of the time of a day students spent in school. There are so many friends created of a student in their school life. School can arrange games, cultural program, creative events along with norms and values. The effect of unethical and unlawful practices on social media should be included in their teaching materials. In class time the use of social media may be restricted without presence of teachers.

Role of religious institution

Everybody should respect religion of own and others. It is a belief which comes from the inner heart of a person. The religious value should be imposes in their minds. Religion institute can try to teach about the bad things and effect of unethical acts on social media and its consequences.

Role of mass media

Now a day mass media can play an important role on any issue. For the betterment of society mass media cannot disagree with unethical and unlawful practices on social media. They can arrange more and more ethical documentary in radio and television. In printing media very nice and attractive ethical article should be published. To create a awareness in the society they can play significant role. They can broadcast about the rules and regulations are prevailing in our country and the penalty of such practices.

IMPLICATIONS AND RECOMMENDATIONS

Nowadays, challenges of cyber security are a threat all over the world. To overcome the challenges every country takes policy and action to do the best for the people and also for the country. The implications of cyber security and social media can play both positive and negative role. Because of a public domain social media can act as a reagent to make a healthy and peaceful society. It can influence the development of a country. On the other hand, it can destroy the image of a country. Sometimes financial corruption and losses may happen. For an individual it may occur depression, suicidal thought, stress, disastrous impact on family reputation and disagreement. The implication of this research work will help the Government to take appropriate measures to provide safe social media filter or block the unethical contents.

The following are the recommendations:

- ☐ The Government needs to activate Digital Security Agency immediately under Digital Security Act'2018.
- ☐ The Cyber Security and Crime Unit of police need to expand all over the country.
- ☐ Government should establish a network monitoring center to filter or block the unethical content of social media for ensuring security at individual to national level.
- ☐ Schools should include effect of social media and its measure in their curriculum.
- ☐ Parental guidance should be friendly and quality time should be spent with children.

CONCLUSION

Cyber security is a core requirement of individuals to national to international level. The study found that the cyber security strategy of Bangladesh is in a vulnerable state, by promoting cyber security education, ongoing risk assessments, counter cybercrime policy, forms of regulation and improvement in Research and Development, Coordination with the International law, Balancing Cyber Security with Civil Liberties and regional cooperation then this can be called as a resilient strategy that is prepared to handle most situations.

The government should take immediate action for reducing the unethical practices on social media by the formulation of a transparent and implementable law. Technological solutions for reducing the unlawful and unethical contents should be deployed immediately. The role of community, parents, government, schools, religious institution and mass media are very significant to control the unethical practices on social media.

REFERENCES

Bangladesh Telecommunication Regulatory Commission (2019) website <http://www.btrc.gov.bd/content/internet-subscribers-bangladesh> (9 September 2019).

Dixon,J, Gulliver,A, Gibbon,D& Hall, M (2001) *Farming systems and Poverty: World Bank*.

Deniel. B (2017) :*Towards a Cyber Security Policy Model – Israel National Cyber Bureau (INCB) Case Study*. (2015, January 07). Retrieved May 24, 2017, from https://publixphere.net/i/noc/page/IG_Case_Study_Towards_a_Cyber_Security_Policy_Model_Israel_National_Cyber_Bureau_INCB

Grant,C&Osanloo, A (2014) *Understanding, Selecting and Integrating a Theoritical Framework*, p-12-22.

International Commission of Jurists (ICJ). (2013). *Briefing Paper on the Amendments to the Bangladesh Information Communication Technology Act 2006*. Retrived 15.06.2014 from <http://icj.wpengine.netdna-cdn.com/wp-content/uploads/2013/11/ICT-Brief-Final-Draft-20-November-2013.pdf>.

Luse, A. Mennecke, B & Townsend, A (2012) *Selecting a Research Topic: International Journals of Doctoral Studies*. P-143-152.

Sarkar. K A (2019) *Comparative Analysis of the Cyber Security Strategy of Bangladesh*: International Journal on Cybernetics & Informatics (IJCI) Vol. 8, No.2, April 2019,p-2-3

The Information & Communication Technology Act, 2006. (2006). the Information & Communication Technology Act, 2006. 39. Retrieved 02.08.2014 from <http://www.prp.org.bd/downloads/ICTAct2006English.pdf>.

The Digital Security Act, 2018.

Williams, B. (2013). *Cyberspace: what is it, where is it and who cares?*.

Retrived 15.07.2014 from <http://www.armedforcesjournal.com/cyberspace-what-is-it-where-is-itand-who-cares/>.

Research Paper Questionnaire

Topic: Use of Social Media

Name:

District:

Age:

Sex: Male ☐ Female ☐

1. Do you use Social Media? Yes ☐ No ☐

2. Which Social Media you visited more/frequently?

Facebook ☐ Whatsapp ☐ Youtube ☐

Viber ☐ Instagram ☐ Others (Please mention)

3. Do you know about the rules, regulation, guidelines to use the Social media?

Yes ☐ No ☐

4. Mention what practices you have ever seen on social media? (Please tick)

Defamation ☐ Vulgar language ☐ Scams ☐

Exclusivity of one's religion ☐ Insulting advertisement ☐

Post against Country or Government or Act ☐ Fake account ☐

Sharing of personal problems ☐ Other (Please specify)

5. What are the effects of unlawful and unethical practices on social media?

* Depression

.....

* Suicidal thoughts

.....

* Stress

.....

* Family reputation

.....

* Disagreement

.....

* Image and Others (please specify)

.....

6. Influence of society on social media's post (Please tick)

Less like ☐ Often ☐ Sometimes ☐ Always ☐

7. Do you think that the malafide/unethical information or contents should be removed/filter from social media before viral?
Yes ☐ No ☐
8. Do you think that the unethical contents like pornography and betting site should be blocked/filter from social media?
Yes ☐ No ☐
9. What can be done to stop the unethical practices on Social Media?
.....
.....
10. What should be the roles of institutions to overcome unethical practices on Social Media?
- * Community
.....
 - * Parents
.....
 - * Government
.....
 - * School
.....
 - * Religious Institution
.....
 - * Mass media
.....

Thank you for your cooperation. All information gathered will be kept confidential.