IOSR Journal Of Humanities And Social Science (IOSR-JHSS)
Volume 25, Issue 3, Series. 8 (March. 2020) 19-28
e-ISSN: 2279-0837, p-ISSN: 2279-0845.
www.iosrjournals.org

Cyber Threat and Security: Bangladesh Perspective

Mahmuda Akhter Bonnya[1]

Abstract: Cyber-crime is now a great threat to cyber security and computer data system in the era of globalization due to the rapid spread of communication and information technology. Even, the technologically advanced countries are not out of the preview of the threat and the developing countries like Bangladesh, which are not technologically advanced enough, are under severe risk of cyber-crimes. Bangladesh government has taken many initiatives under 'Vision 2021' for transforming the country into 'Digital Bangladesh', resulting an accelerated pace of growth of internet users and e-commerce. According to Bangladesh Telecommunication Regulatory Commission, there were 9.13 crore active internet users as of December 2018. Being encouraged with the government's initiatives, many national and multinational companies are facilitating online shopping, banking, and communication and many other e-commerce services. But, the matter of grave concern that most of the software used in the country is pirated. Taking such advantage, criminals take their way in the digital platforms and commit criminal activities through phishing, hacking and stealing of personal and institutional data. More importantly, the terrorist and terrorist organizations conduct their financial and information transactions through using internet.The governmental institutions, private companies and even individuals in Bangladesh become the easy target of cyber criminals, posing a great threat to the country's cyber security. In such scenario, the government's initiatives to combat the cyber-threat and such crimes are very limited. Besides, the country's existing laws to fight the menace are not enough because of those limitations. The article makes use of secondary data such as books, articles and newspaper publications; cyber related different customary laws, Acts and codes of Bangladesh.The article aims to study contemporary the cyber security threat in the global village with an emphasis on Bangladesh along with the existing policies, laws and government's initiatives to combat the threat. The article will also offer policy options for ensuring cyber security.

Keywords: Cyber-crimes, Cyber-security, Globalization, Bangladesh.

Date of Submission: 14-03-2020 Date of Acceptance: 30-03-2020

I. INTRODUCTION

"Cyberspace is the realm of computer networks (and the users behind them) in which information is stored, shared, and communicated outline." (Singer and Friedman, 2014). The age of globalization is marked by the rapid spread of information and communication technology. Secure cyberspace is a key element of protecting national security is the age of globalization. It plays significant role in achieving economic prosperity and credible defense of a country (Williams, 2013). These are important to build a strong, modern, powerful and industrial nation. With the rapid advancement of information and communication technology (ICT), cyber-crime has become a considerable security concern in international area. States are now under security threat from both individual cyber criminals and state sponsored cyber- crimes to protect their confidential data. These threats abysmally impact the economic progress and defense system of a country, and create diplomatic conflict in world order. Thus the issue of information technology hampers the international peace, security and development. The above international

Scenario exacerbates the cyber security of Bangladesh.The country lacks modern information and communication technology that benefits criminals to commit phishing, hacking and stealing of secret private data. Criminals target personal and organizational data, in addition, digital facilities to the general people by government and non-government sectors. Public and private organizations are providing digital facilities without ensuring proper security efforts. Moreover, the Information and Telecommunication Act of the country is ineffective to secure the cyberspace. This study attempts to investigate the major challenges of Bangladesh for its volatile cyber security initiatives in the globalized world. In doing so, the study examined effectiveness of current informational and telecommunication laws, and therefore suggests remedial measures for ensuring cyber

[1] Lecturer, Department of English, City University, Dhaka, Bangladesh and Independent Researcher in the field of Information, Communication and Technology (ICT).
Email:mahmuda1bonnya1@gmail.com

security of Bangladesh. The present study concludes by uttering that it is high time for Bangladesh to secure its cyber space in order to emerge as a powerful state in the world.

II. CYBER SECURITY IN THE GLOBAL VILLAGE

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. Cyber threat generally appears as a form of cybercrime that can harm individuals or specific target groups or organizations or even a state actor itself. The cyber criminals tend to look for scopes to attack at networks, systems, data and operators for financial gains. B. Williams described that criminals generally approach four types of cyber-crimes. First, who are just after the money. Such example of this occurred in April 2013 when U.S. stock market faced an amount of $130 billion within minutes just because of a hacked Tweeter newsfeed propagated a false report of an explosion at the White House (Williams, 2013). Secondly, ones are the competitors, searching for critical information or intellectual property that may provide them edge to other. It is equally concerning matter for both civilian and defense sectors. Recently, a Russian crime organization cumulated the largest known collection of stolen internet data consists of 1.2 billion user name and password combinations, more than 500 million email addresses (Perlroth, Gellesaug, 2014). Third is the threat posed from inside either from an insider de facto or lack of proper security precautionary measures.Ranging from Iran's nuclear facilities to thousands of American diplomatic cables, recent high profile breaches of IT systems have highlighted the growing importance of cyber-security for this Information Age. Cyber-crime crosses national boundaries, and the issue is further exacerbated by the anonymity of attackers and the disproportionate potential for damage. While a notable problem in its own right, cyber-crime presages the inevitable conflicts that will arise from the close contact afforded by the internet between varying cultural norms. The advent of the Information Age has enabled unprecedented connectivity between not only individuals around the globe, but also connectivity across organizational scales. Large governments and corporations may quickly – and cheaply–directly reach and be reached by almost anyone with Internet access, as information transmission to even to non-networked systems is greatly facilitated by common software platforms used throughout the world. Such access, while beneficial to all, comes at a potential price.

Worldwide governments and organizations are, in the face of increasing numbers of cyber security incidents, turning their focus to how to manage cyber security threats and deal with the aftermath of cyber security incidents. For many organizations, the most common cyber security threat is the risk of confidential information being accessed and potentially misused by an external and/or adverse party i.e. data breaches. One of the key challenges in responding to data breaches is that data can be taken from one or more jurisdictions, and moved very quickly to other jurisdictions. The cross border nature of incidents can make investigating a data breach, identifying your various obligations in relation to the data breach and identifying your options for dealing with the data breach, a very complex and daunting process. This is especially so because speed is almost always a critical factor in an effective response. In the Asia Pacific region, recent years have seen a wave of new cyber security legislation, government established bodies to regulate or monitor cyber security and guidelines/reports being issued by governments and regulators. For example, in 2015, Indonesia and Singapore each introduced cyber agencies, Japan enacted the Cyber Security Basic Act and the Australian Securities and Investments Commission released a report on cyber resilience. For a number of countries in Asia Pacific, laws or guidelines on these issues are being formulated for the first time. In addition, countries such as the United States, where the Department of Justice released in April 2015 its "Best Practices for Victim Response and Reporting of Cyber Incidents", are adding to already existing systems of cyber security regulation. Despite the increased regulatory activity, there is, unfortunately, no unified approach to the regulation of cyber security or the potential legal remedies available in the context of data breaches in the Asia Pacific region. Depending on the jurisdiction, data breach incidents may involve, in addition to laws regarding cyber security, obligations under privacy laws, employment/labor laws, equitable rights and obligations, the law of equity, corporate governance, fiduciary duties and industry or sector specific regulations. In some jurisdictions, laws regarding state or national secrets may also be enlivened, especially when data is suspected to have been transferred out of the jurisdiction. Accordingly, local knowledge of the obligations in each country and how each relevant regulator or court operates in practice is essential to navigating a response to a data breach incident and understanding which legal remedies may be available and which will be most effective. Using this knowledge, it is able to assist the clients to investigate data breaches, to identify reporting obligations, to discuss strategies to minimize further disclosure of the data and mitigation of loss or damage, and to identify, where available, legal remedies to recover the data or loss associated with the data breach.

Many of the websites of Bangladesh government use foreign servers and foreign vendors. As a result, these are always in vulnerable position and at risk to be sabotaged by the insiders of the system (Alam, Md. Shah, personal communication, July 27, 2018). The fourth approach is potentially the greatest threat to our national security. This is regarding state-sponsored cyber- attack to weaken a national security system such as critical infrastructure or essential national economic components to a certain level for gaining strategic

advantages over that particularly affected country (Williams, 2013). In this case, the example of China can be mentioned. China always regarded as a potential candidate who posed cyber security threat to other influential countries such as U.S., U.K., France, Germany, and India etc. for gaining strategic advantages. In 2007, it was claimed that China launched a series of network-based cyber- attacks against the above mention countries. In fact, these countries have larger military ambitions as well to improve the country's ability to engage information or cyber warfare if needed in near future (Greenemeier, 2007). It can now easily comprehend the global vulnerability and complexity of cyber security matter around the globe. No one is safe from anyone and anyone can be affected from anybody.

III. CURRENT SCENARIO OF CYBER SECURITY IN BANGLADESH

The world is becoming more and more globalized thanks to the rapid growth of information and communication technology especially due to internet. Bangladesh is also trying to be an active participant in this evolution. Due to lack of adequate natural resources, the country is trying to achieve economic independence through the utilization of ICT industry. Moreover, Bangladesh intends to use ICT sector as boosting element for socio-economic development (Maruf, Islam, Ahamed, 2010, p. 118). The Awami League-led present government of Bangladesh has taken vision-2021. It's another interpretation is Digital Bangladesh vision. Bangladesh wants to be fully digitalized in every national sector such as educational institutes, hospitals, financial institutes, law-enforcement agencies, service sectors, etc. Private sectors are also coping with the pace as well such as offering online services to consumers, facilitating online shopping, e-commerce, e-banking, mobile banking etc. As like every thesis has an anti-thesis, vision for digitalized Bangladesh has its adverse effects also. With the increasing online activities in cyber space, criminals are using this space as well for their own criminal activities. In the process of becoming a digitalized country, phishing, hacking, and stealing of personal data are routine activities in Bangladesh (Bleyder, 2012). If we examine the nature of cyber-crimes, then we have a clear picture of cyber security condition in Bangladesh. We can see two broad categories of cyber-crimes in Bangladesh, direct and indirect. Direct cyber-crime nature in Bangladesh is almost similar to world context such as malicious mail to foreign diplomatic mission and other VIP personnel, pornography, use of e-mail for illegal activities, use of internet for transmitting false and malicious information, use of internet for prostitution (a lot of examples of illegal prostitution promotion web sites of Bangladesh), use of internet for women and child trafficking etc. (Alam, 2007). On the other hand, indirect cyber-crimes are like pathways for traditional crimes such as kidnapping, robbing banks, committing murders, threatening and demanding money by using exclusive pornographic videos and pictures (photo-shopped in most cases) etc. According to Bangladesh Police, the traditional crime rate has decreased significantly compare to 80s and 90s but in reality the criminals are using new risk free methods to conduct the crimes and in these cases indirect use of cyber-crimes are the most preferable methods. Cyber-crimes may still not that much popular as replacement for traditional criminal activities in Bangladesh but these are using as medium of various kinds of organized crimes. In recent months, the rates of these indirect cyber-crimes have increased rapidly. Bangladesh Police investigated such a crime where an interesting case came up. A consultancy agency gave advertisements in prominent national dailies such as *ProthomAlo* by saying that they can send Bangladesh citizens to Canada and interested candidates need to pay 16.5 Lac (1.65 million) taka for that. The case seemed unusual to police and they went to investigate to that particular company named 'BD Company.' Later on police found out it's a fraud company without adequate knowledge and government approval or license for manpower business. The company's Managing Director (MD) is a young person and never visited any country before. This seemed a regular crime at first but in reality it was part of an international organized crime and young MD was just a pawn of it. He was also played in the hand of an international organized crime network. At the time of investigation already 37 interested candidates paid one Lac (100 thousand) taka per each to that company just because of the lack of awareness, and the young MD sent 26.5 Lac (2.65 million) taka to his counterpart by using Hundi (did not pay government tax using illegal means) to another Bangladesh citizen living in UK and he deposited it to the original suspect's bank account. This money laundering process used internet and online banking system very frequently and the prime criminal suspected to be a citizen of Nigeria who has international bank account in UK. In this case, we can clearly assume how cyber-crime can be used in the process of traditional criminal activities (Alam, Md. Shah, personal communication, July 27, 2018).

IV. CYBER VIOLENCE AGAINST WOMEN IN BANGLADESH:

Women in Bangladesh are disproportionately targeted by online and technology facilitated violence and harassment. While the expansion of Information and Communication Technology (ICT) and growing internet penetration are considered as positive indicators of development in the country, but their interaction with certain pre-existing social-physiological settings related and inadequate legal protections have led to increased cyber violence against women. In most cases, the form of this glaring violation of human rights ranges from cyber stalking, revenge porn, cyber bullying, and trolling. Women are the primary recipient of

offensive and often aggressive sexual advances and defamatory messages in cyberspace from anonymous and fake sources. False and altered unclothed pictures of women along with spam, sex-act videos, rape threats, and indecent proposals have become the new norm of social media. Women are the primary recipient of offensive and often aggressive sexual advances and defamatory messages in cyberspace from anonymous and fake sources. False and altered unclothed pictures of women along with spam, sex-act videos, rape threats, and indecent proposals have become the new norm of social media.

Access to internet in Bangladesh is growing very rapidly through mobile telephony; the total number of internet subscribers has reached 85.918 million at the end of April, 2018. More the 93 percent of these subscribers use internet on mobile phones, rest of them are ISP [Internet Service Provider] or PSTN [Public Switched Telephone Network] users (Bangladesh Telecommunication Regulatory Commission-BTRC, 2018). As of April, 2018 total number of people using mobile phones are more than 150 million (BTRC, 2018). With this proliferation of internet and mobile phones, use of social media platforms has been increased, 29 million registered Facebook users of which 86 percent use Facebook from their mobile devices. At least one third of the subscribers of mobile phones and internet are women. Access to internet in Bangladesh is growing very rapidly through mobile telephony; the total number of internet subscribers has reached 85.918 million at the end of April, 2018. At least one third of the subscribers of mobile phones and internet are women. In Bangladesh, particularly young women are more likely than men to face severe online abuse that is sexualized and violent. In spite of weak institutional protection, women often make formal report of harassment, abuse, and violence originated from online spaces. According to a study, 73 percent of women internet users have reported cybercrime (Zaman, Gansheimer, Rolim, &Mridha, 2017). As of December, 2017 the government's Information and Communication Technology Division's Cyber Help Desk has received more than 17,000 complaints, 70 percent of complainants were women.

As of December, 2017 the government's Information and Communication Technology Division's Cyber Help Desk has received more than 17,000 complaints, 70 percent of complainants were women.Unwanted and wanted exposure of online pornography among the young population led to other associated risks such as image-based abuse of users where women are highly disproportionately targeted. In 78% of these cases related with digitally manipulated images with pornographic materials, the victim is found to be a woman. It may be noted that, almost 77% of the country's teenagers watch pornography on a regular basis (MJF, 2014). Bangladesh National Woman Lawyers' Association noted in June, 2017 that harassment remained a problem and monitoring and enforcement of the guidelines were poor, which sometimes prevented girls from attending school or work. The formation of complaints committees and the installation of complaints boxes at educational institutions and workplaces required by the Court's directive were rarely enforced (USSD, 2017). Often women end up with their social media accounts hacked. The perpetrators would then upload fake, undressed pictures of the victim to victimize them. Also, indecent messages are sent from her account to her contacts (i.e. Facebook friends) to undermine and dishonor the victim. Among the key motives of such cyber-crimes against women are defaming the victim; revenge; compelling the victim for physical relation; blackmailing for money; physiological torture; ego and power trips; the obsession for love and emotion etc.

Among the key motives of such cyber-crimes against women are defaming the victim; revenge; compelling the victim for physical relation; blackmailing for money; physiological torture; ego and power trips; the obsession for love and emotion etc. A quick review of the lawsuits, investigations and media reports reveal a somewhat common pattern among most of the cases of cyber violence against women in Bangladesh. Quite often heinous acts of rape are recorded in the form of video and photographs by the criminals. They then go on to use these to silence the victim. But it doesn't end just there. Most often, these recordings are used to keep forcing the victim into submission – to keep having physical relationships, blackmailing for money etc. In another pattern we notice, the perpetrators take their time to gain the trust of their victims. They then convince their prey to have the physical relationship in a supposedly safe place (i.e. hotel rooms, friend's home) where hidden cameras are set up beforehand. After their intimate moments are recorded, these are used to blackmail the victims if they don't submit to the will of the perpetrators. As usual, these recordings are released on the internet nonetheless. Another common pattern is posting of intimate photographs and videos by ex-husbands and lovers on the internet as a means of revenge. Young girls who are newly introduced to the internet and are rather inexperienced in the cyber world are consequently most susceptible to falling into the traps set by cybercriminals.

4.1Effects of cyber violence

In a somewhat conservative society like Bangladesh, the effects of cyber violence against women are not limited to the victims. They have a chain reaction on their families and eventually tear a hole in our social and moral fabric.It has been observed that most people generally believe everything posted in social media.Lack of awareness, ignorance and education results into a shallow public psychology which is a major reason for such indiscriminate belief system. As a result, when a girl's exposed photographs are published along with a spicy

fabricated story, general internet users do not go into analyzing whether it's true or false. They are rather happy to consume such content and become interested to spread the gossip. Such tendency helps make almost any kind of online sex-related chatter go viral thereby amplifying the victim's suffering by a thousand times. Not to mention the misery of the victim's family members who face social exclusion, humiliation and public resentment (Karaman, 2017).In a somewhat conservative society like Bangladesh, the effects of cyber violence against women are not limited to the victims. They have a chain reaction on their families and eventually tear a hole in our social and moral fabric.At an individual level, such cyber violence lead to severe depression, guilt, embarrassment, self-blame apprehension and fear of harm to self and family members. Consequently, it leads to shattering the victim's career, education and social life. Some victims take the route of drug addiction while some choose to end their lives. Only in a handful of exceptional cases do we see the victims recover from such a tragedy.From 2010 to 2014, Bangladesh National Woman Lawyers' Association identified a total of 65 reported suicide attempts by female victims of violence. It also reveals that on an average, every year there are 11 suicide attempts by women due to cyber violence. By contrast, in 2008 this number stood at 8 revealing a sharp increase in the trend. Needless to mention, the official statistics is just the tip of the iceberg. The number of unreported cases far outweighs the reported ones (BNWLA, 2014). Every year there are 11 suicide attempts by women due to cyber violence.

V. CHALLENGES TO BANGLADESH

When anyone starts to think about cyber security in Bangladesh, the words stuck in mind that are 'pirated software' and poor infrastructural system to protect cyber space in Bangladesh. In Bangladesh, around 90% of software is pirated (Bleyder, 2012). Using pirated software has become a culture and habit to Bangladesh people. This habit of using pirated software is leading us to more vulnerable position in the cyber security domain. This is the only challenge that Bangladesh is facing right now in the quest of cyber security but it can't ignore the impacts and consequences of it either. Apart from security concern regarding pirated software uses, there are some grave challenges as well regarding Bangladesh cyber security that we cannot deny anymore. To understand the challenges of cyber security in Bangladesh, first it is needed to be aware of the nature of cyber-crimes in Bangladesh that we are facing day to day life. It can divide it into four categories. First, cyber-crimes that are targeting individuals, such as: hacking or cracking, illegal/unauthorized access, illegal interception, data interferences, E-mail spoofing, spamming, cheating and fraud, harassment and cyber stalking, defamation, drug trafficking, transmitting virus and worms, intellectual property crimes, computer and network resources vandalism, internet time and information thefts, forgery, denial of services, dissemination of obscene material etc. Second one is cyber-crime against property such as: credit card fund stealing, intellectual property crimes, internet time theft etc. Third one is crime against organizations. Such crime examples are like unauthorized control/access over the network resources and websites, exposing indecent/obscene materials over the web pages, virus attack, E-mail bombing, logic bombing, Trojan horse, data diddling, blocking from access, theft of important possessions, terrorism against government organizations, vandalizing the infrastructure of the network etc. Fourth and last categories of cyber-crimes are happening against the society or social values of Bangladesh. Such crimes are like forgery, online gambling, trafficking, pornography (especially child pornography), financial crimes, polluting the youth through indecent exposure, web jacking etc (Maruf, Islam, Ahamed, 2010).

Discussing the major challenges for cyber security in Bangladesh, pornography is a concern for Bangladesh especially if we consider the social values, morals, ethics of Bangladeshi culture and society. We can now chat with anyone in the globalized world. We can share and exchange our cultural values. A very natural element of different country's culture may harm our culture heavily because of cultural diffusion. Spreading of pornography is such a bothersome element for Bangladeshi culture where not even adult education has not been accepted yet. According to Bangladesh Police, they are facing many cases where people are regularly demanded to give ransom money or conned by illegal pornographic use such as secret nude video footage, photo-shopped pornographic picture editing etc. Criminals are targeting victims' closed ones like parents, family members, relatives etc. Victims can be any woman or child even boy child as well but the frequency of teenage girls victims are higher than usual. In this regard, we must consider the 'duel criminality' as well. Duel criminality means that the crime has been acknowledged in both countries of victims and crime suspects and here lays another complexity to deal with pornography. Usually in many countries such as in U.S., adult pornography may not be a crime in every case but in Bangladesh it is so when the crime suspect is related to U.S. then Bangladesh cannot claim it as duel criminality and faces difficulties to deal with this crime as transnational crime itself is a complex issue. On the other hand, child pornography is a duel criminality, and we can work together through international cooperation. We can give an example in this case. In this year, a famous litterateur for writing child-literature in Bangladesh named TipuKibria had been caught in red hands of police for illegal child pornographic activities. He used street male children for making child pornographic videos and photo shooting in his home and lab. At the time when he was caught by the police, he had already abused

around 400-500 street children for his dirty ambition. He has two assistants to help him out in these illegal activates and police found 13 international buyer names from TipuKibria who regularly paid him for weekly supplies through international or online bank transactions. Bangladesh Police also suspects that maybe there are many more suppliers other than TipuKibria as well. So we can clearly say, pornography is a serious concern regarding Bangladesh cyber security concern (Alam, Md. Shah, personal communication, July 27, 2018).

Cyber security threat regarding financial transaction such as online banking, e-commerce, money laundering, financing to transnational organized crimes like drug trafficking, terrorism etc. are another major challenge to Bangladesh cyber security arena. Cyber threat can lead Bangladesh to serious economic downfall especially in banking sector. Bangladesh is a new customer of online financial transaction and lack proper maturity in this new field but a globalized world is making online banking and any kind of online transaction more frequent so Bangladesh cannot deny the inevitable consequences as well. As a result, it is going to become a major security concern in upcoming days. Widespread uses of credit cards and the rise of electronic payment methods are also putting a large number of customers' private information such as bank account name, bank account number, cell number, E-mail ID etc. in danger (Bleyder, 2012). In recent times, Bangladesh law-enforcement agencies are facing many cases regarding direct or indirect cyber threats to Bangladesh online banking sector or other online financial transactions. Bangladesh Police described one particular case where a single individual person held 125 credit cards in his name from 5-7 different banks. At the time of his capture, there had already been millions taka dealing through these credit cards. In these cases, internal employees of banks are also involved and they are promoting these activities for getting profit sharing. In the name of fake companies, millions of taka has been vanished from banks and online banking, credit cards are now the safest and preferable ways to do that. Banks are taking many security initiatives to restrict illegal transactions but internal sabotage and security dependency on others are making it more challenging. On top of that, after revealing money laundering or forgery, banks usually do not want to take proper responsibilities and try to hide the case for considering their age old reputation. The most troublesome condition in this case is that banking authority often tries to make their innocent customers as shadow victims by accusing them as a faultier for these financial misconduct and it turns into a cause of individual security concern. Apart from sabotaging online financial transaction, there are always threats of phishing as well. Phishing or pulling out confidential information from the bank/financial institutional account holders by using deceptive means or provocative e-mails, advertisements are affecting a large of victims in Bangladesh. In these cases, victims usually lose 100-500 USD per case and they hesitate to go to the police for complaining which again make the case more difficult to tackle for law-enforcers in Bangladesh (Alam, Md. Shah, personal communication, July 27, 2018).

Hacking or illegal intrusion into a computer system without the permission of owner or user (Maruf, Islam, Ahamed, 2010, p. 116) is another prime concern of Bangladesh cyber security especially for disrupting good diplomatic relations with other countries and creation of confusion among various parties. Hacking has become a routine security concern in Bangladesh nowadays. Usually government and important financial institution websites are the targets of hackers. In the name of ultra-patriotism or ultra-nationalism, a country's young hackers can attack another country's website and it may enter into a void of attack and counter attack collision. Lack of adequate cyber security knowhow, poor cyber infrastructural system such as dependency on outside server system provider companies etc. are putting Bangladesh in more difficult position to combat cyber hacking (Alam, Md. Shah, personalCommunication, July 27, 2018). Another major challenge for Bangladesh cyber security is data stealing. Such recent example is the issue of leakage of partial verdict of Bangladesh War Crime Tribunal before having a formal court's decision. This was happened through Skype voice recording. It was a major backlash for Bangladesh government and exposed the vulnerability of Bangladesh cyber security arena (Alam, Md. Shah, personal communication, July 27, 2018).

Apart from above challenges, there are cyber security threats to individual level as well. A scene of personal insecurity is always working nowadays in Bangladesh because of the rapid growth of internet and social network such as Facebook. Anyone can be victim and feel insecurity of losing personal information or facing unwanted threats that can demolish his/her respect and social prestige within a matter of time. At the end, we cannot say cyber-crime or internet based crime is not just a part of routine crime anymore in Bangladesh rather it is spreading to a more complex form of crime where traditional criminals are using cyber space in a more covert and smarter way to do their job.

VI. EXISTING ACTS AND THEIR LIMITATIONS

In the context of cyber security, the only legal structure in Bangladesh is 'The Information & Communication Technology Act, 2006' or shortly known as ICT Act 2006 which was initiated on 08 October 2006 (ICT Act, 2006). Bangladesh Parliament amended this ICT Act on 06 October 2013. The law enforcement agencies are suggesting this is a good law to combat cyber-crimes in Bangladesh as a victim of cyber-crime can file a case against the criminals under this law no matter where the criminals are in the world. The victims can use this ICT Act at least to move as an starter though after that they definitely need good cooperation to progress

from first, specific Bangladesh law enforcers who have expertise regarding cyber security such as CID (Criminal Investigation Department) and secondly, from international law enforcers such as Interpol (Alam, Md. Shah, personal communication, July 27, 2014). The amendments of ICT Act 2006 that have been initiated in 2013 created many ruckuses under the Act non-bailable and cognizable. '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 mentioned objective of the ICT Act is 'the legal recognition and security of information and communication technology'. After the amendments with few significant changes, the main Act of 2006 remains unchanged with all its discrepancies and imposed unnecessary harsh punishments (Barua, 2014). However, after being amended, the ICT Act 2006 has become a tool of Bangladesh government to violate basic human rights such as freedom of opinion and expression. If we analyze the original ICT Act, it contains a number of vague imprecise and overboard provisions that may help to instigate cyber-criminal acts further rather than containing. Section 57 (1) of the original Act stated as such, "If any person deliberately publishes or transmits or causes to be published or transmitted in the website or in electronic form any material which is fake and obscene or its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, or causes to deteriorate or creates possibility to deteriorate law and order, prejudice the image of the State or person or causes to hurt or may hurt religious belief or instigate against any person or organization, then this activity of his will be regarded as an offence" (ICT Act, 2006). According to the section 57 of original ICT Act is 'incompatible with Bangladesh's obligations under article 19 of the ICCPR: the offences prescribed are vague and overbroad; the restrictions imposed on freedom of opinion and expression go beyond what is permissible under Article 19(3) of the ICCPR'. In this regard J. Barua said, "Section 57 is not specific and covers a wide area of offences, there will be little chance to get acquittal from any charge" (Barua, 2014). After analyzing the ICT Act 2006 with its amendments, we can say that there should be law to contain crimes related to cyber space but the existing act is vague and need to be designed as modernistic legal framework in a permanent basis not just rely on ad-hoc framework (Editorial, The Daily Star, 2013).

Besides the ICT Act, 2006 the Digital Security Bill 2018 was passed in parliament on September 19, 2018 allowing police officials to search or arrest anyone without any warrant. The bill got through by voice vote amid opposition from a number of Jatiya Party lawmakers, ignoring concern of journalists, owners of media houses and rights activists over some of its sections. Section 43 of the new law says if a police official believes that an offence under the law has been or is being committed at a certain place, or there is a possibility of committing crimes or destroying evidence, the official can search the place or any person there. Section 3 of the new law includes a provision of the Right to Information Act 2009, which will be applicable in case of right to information-related matters. As per section 32 of the law, if a person commits any crime or assists anyone in committing crimes under Official Secrets Act, 1923, through computer, digital device, computer network, digital network or any other electronic medium, he or she may face a maximum 14 years in jail or a fine of Tk 25 lakh or both.The law also includes a definition of the "Spirit of the Liberation War" in section 21, which says, "The high ideals of nationalism, socialism, democracy and secularism, which inspired our heroic people to dedicate them to, and our brave martyrs to sacrifice their lives in, the national liberation struggle."According to section 29 of the law, a person may face up to three years in jail or a fine of Tk 5 lakh or both if he or she commits the offences stipulated in section 499 of the Penal Code through a website or in electronic form.Section 31 of the act says a person may face up to seven years in prison or Tk 5 lakh in fine or both if he or she is found to have deliberately published or broadcast something on a website or in electronic form which can spread hatred and create enmity among different groups and communities, and can cause deterioration in law and order.

7. Policy Opinions

In the above scenario, we can offer several remedial policy options regarding cyber security, cyber space protection and minimizing the cyber-crime rates in Bangladesh. We are mainly recommending policy options for Bangladesh government but it also includes individual security domain as well. These options could be as such:

7.1. Reform of Legal Structure

We are echoing ICJ's policy recommendations to both Bangladesh Parliament and Bangladesh Government regarding ICT Act 2006 and its amendments. ICJ calls the Bangladesh Parliament as such, 'Repeal the Information and Communication Technology Act (2006), as amended in 2013, or to modify the ICT Act to bring it in line with international law and standards, including Bangladesh's legal obligations under the ICCPR. At a minimum, this would require that it, (1) Amend section 57 of the ICT Act so as ensure any contemplated restrictions on freedom of opinion and expression are consistent with international law and standards; (2) Amend section 57 of the ICT Act to ensure prohibited expression is clearly defined; (3) Amend the ICT Act to ensure that any restriction to freedom of expression and information, including any sanction provided for is

necessary to a legitimate objective and proportionate to the harm caused by the expression' (ICJ, 2013). ICJ also recommended policy options to Bangladesh Government in this regard. Such policy options are, (i) 'Take steps to ensure that provisions of the ICT Act are not used to violate the right to freedom of expression, including to limit the legitimate exercise of comment on public matters which might contain criticism of the Government; (ii) Drop charges against bloggers for the legitimate exercise of their freedom of expression; (iii) Direct Government agencies to desist from filing politically motivated cases unlawfully restricting the exercise of expression, as well as and seeking penalties which are disproportionate to the gravity of the alleged offence' (ICJ, 2013).

7.2. Maintaining Rules of Cyber Security

In 2011, EnekenTikk, the Legal Advisor at the NATO Cooperative Cyber Defense Centre of Excellence, Tallinn, Estonia, provided a conceptual framework of maintaining rules of cyber security considering both national security issues and individual liberty security concerns in his article 'Ten Rules of Cyber Security.' We are also agreeing with EnekenTikk in many cases. He talked about 'the territorial rule' protecting cyber security as such, "Information infrastructure located within a state's territory is subject to that state's territorial sovereignty" (Tikk, 2011, p. 121). Tikk also talked about 'the responsibility rule' where he suggested to the states to act responsibly to protect their own territory. He also told about 'the early warning rule' as such, "There is an obligation to notify potential victims about known, upcoming cyber-attacks" (Tikk, 2011, pp. 122-126). By analyzing Tikk's above cyber security rules, we can recommend a strong national cyber intelligence agency for Bangladesh to combat current and upcoming potential cyber threats from anywhere of the world as prevention is better than cure. Secondly, according to Tikk, a state should protect its important national data implying 'the data protection rule.' He clearly stated, "Information infrastructure monitoring data are perceived as personal unless provided for otherwise." In this regard we can also mentionTikk's another rule, 'the duty to care rule.' He is suggesting everyone to take a minimum level of responsibility to secure any kind of information infrastructure (Tikk, 2011). By echoing his thought, we can suggest Bangladesh Government to utilize our own resources, expertise and initiate advanced technology to protect our cyber space and national interest. Proper training to our cyber experts, developing own server systems and networks using our own resources and manpower, spending quality time to develop our cyber security safety net, recruiting promising young national hackers of Bangladesh etc. can be beneficiary in the long run rather than relying on foreign experts. Thirdly, we can agree with 'the cooperation rule' of Tikk. He stated that, "…cyber-attack has been conducted via information systems located in a state's territory creates a duty to cooperate with the victim state" (Tikk, 2011, p. 123). We need a strong international cooperation to battle any kind of cyber security threat as most of the cases, these threats have been involved with transnational criminal activities where victim may be victimized in one country and criminals may run away by taking advantages of international border barriers. Bangladesh Government and Bangladesh Police have already been in touch with international law enforcer such as Interpol in this regard but Bangladesh needs more cooperation especially from the tech giants such as Microsoft, Google, Facebook, Yahoo and others. Lastly, we can refer Tikk's another two rules regarding 'the self-defense rule' and 'the access to information rule.' He said that, "everyone has the right to self-defense" and "the public has a right to be informed about threats to their life, security and well-being" (Tikk, 2011). By quoting him, we are also suggesting that Bangladesh Government should consider about the personal information safety and precautionary measures taken for the well-being of Bangladeshi citizens along with protecting national cyber security.

7.3. Individual Awareness

We cannot ignore the consequences of globalization anymore. Apart from our government it is also the duty of every individuals of Bangladesh to consider the safety of his/her personal data and information. In both public and private sectors, the top management, the middle management and ground level service providers, employees, employers, workers, students, customers, consumers etc. should have minimum level of education and expertise to handle the cyber technologies. They should be aware of cyber threats as well. Only proper education and awareness can rescue Bangladesh from falling into deep pitfall of cyber security threats (Alam, Md. Shah, personal communication, July 27, 2018).Anyone using the internet should exercise some basic precautions. Here are 11 tips which may help protect us against the range of cybercrimes out there. (i) To use a full-service internet security suite, (ii) To use strong passwords (iii) To keep your software updated (iv) To manage the social media settings (v) To strengthen home network (vi) To talk to your children about the internet (vii) To keep up to date on major security breaches (viii) To take measures to help protect yourself against identity theft (ix) To know that identity theft can happen anywhere (x) To keep an eye on the kids and (xi) To know what to do if you become a victim.Ifanyone believe that s/hehasbecome a victim of a cybercrime, s/he needs to alert the local police and, in some cases, the FBI and the Federal Trade Commission. This is important even if the crime seems minor. His/her report may assist authorities in their investigations or may help to thwart

criminals from taking advantage of other people in the future. If we think cybercriminals have stolen our identity. These are among the steps we should consider.

- Contact the companies and banks where you know fraud occurred.
- Place fraud alerts and get your credit reports.
- Report identity theft to the FTC.

VII. 8CONCLUSION

Overall, in the globalized world, cybercrime can pose potential threat for the national security of any country whereas Bangladesh is more vulnerable to this type of threats. Because of the lack of advanced cyber technologies and lack of awareness, the country can suffer extreme security threat produced by cyber-crimes. Moreover, the existing acts regarding cyber space are not effective to safeguard the cyber space of the country. Bangladesh needs more international cooperation, technical knowhow and expertise and massive public awareness to deal with cyber security threat and its use in transnational organized crimes. Many of us can argue that the cyber threats may not be the possible near future scenario for Bangladesh but we cannot ignore the existing facts regarding the increase of cyber-crimes in both Bangladesh and global world. Finally, it can be concluded that, it is high time for Bangladesh to initiate proper measures to combat any potential threat committed by cyber criminals. In this case, the government of Bangladesh and the general people can take into consideration the above suggestions provided in this paper respectively.

REFERENCES

[1]. Alam, Md. Shah. (2007). *Cyber Crime: a new challengen for law enforcers!*.

[2]. Retrieved on 19.06.2014 fromhttp://www.prp.org.bd/cybercrime_files/Cybercrime%20--%20Bangladesh%20Perspective.ppt.

[3]. Barua, J. (2014). Amendment Information Technology and Communication Act. *TheDaily Star.* Retrived on 02.08.2014 from http://www.thedailystar.net/supplements/amended-information-technology-and-communication-act-4688.

[4]. Bleyder, K. (2012). *Cyber Security: the emerging threat landscape* (Issue 10). Dhaka: Bangladesh Institute of Peace and Security Studies.

[5]. BNWLA. (2014). Survey on Psychological Health of Women. Dhaka: Bangladesh National Women Lawyers' Association.

[6]. BTRC. (2018, April 30). Internet Subscribers. Bangladesh Telecommunication Regulatory Commission: http://www.btrc.gov.bd/content/internet-subscribers-bangladesh-april-2018.

[7]. Editorial. (2013). Draft ICT (Amendment) Ordinance-2013: a black law further blackened. *The DailyStar.* Retrieved on 02.08.2014from

[8]. http://archive.thedailystar.net/beta2/news/draft-ict-amendment-ordinance-2013/.

[9]. Greenemeier, L. (2007). *China's Cyber Attacks Signal New Battlefield Is Online.*Retrieved on 15.07.2014 from http://www.scientificamerican.com/article/chinas-cyber-attacks-sign/.

[10]. The Information & Communication Technology Act, 2006. (2006). *The Information &Communication Technology Act, 2006.* 39. Retrieved on 02.08.2014 fromhttp://www.prp.org.bd/downloads/ICTAct2006English.pdf.

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

[12]. Karaman, S. (2017, 11 29). Women support each other in the face of harassment online, but policy reform is needed. The LSE Women, Peace and Security blog. London: The London School of Economics and Political Science. http://blogs.lse.ac.uk/wps/2017/11/29/women-support-each-other-in-the-fa...

[13]. Maruf, A. M., Islam, M. R., Ahamed, B. (2010). Emerging Cyber Threats in Bangladesh: in quest of effective legal remedies. In Editor A. W. M. Abdul Huq (ed.), *TheNorthernUniversity Journal of Law*. Dhaka: Northern University Bangladesh.pp. 114-118.

[14]. MJF. (2014). Report on Porn Addicted Teenagers of Bangladesh. Dhaka: ManusherJonno Foundation.

[15]. Perlroth, N., Gellesaug, D. (2014). *Russian Hackers Amass Over a Billion InternetPasswords.* Retrived 12.07.2014 fromhttp://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internetcredentials.html?action=click&contentCollection=Asia%20Pacific&module=MostEmailed&version=Full&region=Marginalia&src=me&pgtype=article&_r=0.

[16]. Singer, P. W., Freidman, A. (2014). *Cybersecurity and Cyberwar: what everyone needs to know.* Oxford: Oxford University Press. p.13.

[17]. *The Daily ProthomAlo*, 6th October, 2015.
[18]. Tikk, Eneken. (2011). Ten Rules for Cyber Security. *Survival: global politics and strategy*. (p. 119-132). London: Routledge.Pp.124-127.
[19]. USSD. (2017). Country Report on Human Rights Practices for 2016. Washington DC: US Department of State. Available at
[20]. https://www.state.gov/j/drl/rls/hrrpt/2016humanrightsreport/index.htm?ye...
[21]. Williams, B. (2014). *Cyberspace: what is it, where is it and who cares?*. Retrieved on 15.07.2014 from http://www.armedforcesjournal.com/cyberspace-what-is-it-where-is-it-and-who-cares/.
[22]. Zaman, S., Gansheimer, L., Rolim, S. B., &Mridha, T. (2017). *Legal Action on Cyber Violence Against Women*. Dhaka: Bangladesh Legal Aid Services Trust (BLAST). https://www.blast.org.bd/content/publications/Cyber-violence.pdf

Mahmuda Akhter Bonnya. "Cyber Threat and Security: Bangladesh Perspective" *IOSR Journal of Humanities and Social Science (IOSR-JHSS)*, 25(3), 2020, pp. 19-28.