International Journal on Emerging Technologies **11**(5): 425-431(2020)

ISSN No. (Print): 0975-8364
ISSN No. (Online): 2249-3255

Cyber Security and its Reality in Bangladesh: An Analysis of Existing Legal Frameworks

Kudrat-E-Khuda (Babu)

Associate Professor, Department of Law, Daffodil International University, Dhaka, Bangladesh.

(Corresponding author: Kudrat-E-Khuda (Babu))
(Received 10 August 2020, Revised 16 September 2020, Accepted 05 October 2020)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: With the rapid penetration of the Internet and other information and communication technology worldwide, cyber-crime is emerging as a threat to personal data stored in computers and likely to affect the entire data systems. Even the United States, one of the most technologically advanced countries, is also subjected to such crimes. Bangladesh, being a less developed country, is also under the risk of cyber-crimes that might jeopardize the country's national security. As the incumbent government eyes to ensure internet connectivity at all government institutions by 2021 upholding the motto of 'Digital Bangladesh', more and more national and multinational companies are offering online services to their services through the internet following the government's agenda. From shopping to Banking, all are just a click away with the higher rate of internet penetration. However, criminals are also using the online platform where they are committing various sorts of criminal activities including phishing, hacking, and stealing personal data. Hence, the state-owned, as well as private organizations, might fall prey to cyber-attacks which might affect the lives of the entire population. More importantly, there have been scores of media reports saying that terror groups use the online platforms for financing and maintaining intra-group communications. In this context, the existing laws and government moves against cyber-crimes are apparently very scanty to combat the burgeoning threat. There was no funds to conduct the study and to get the cybercrimes related information from the governmental offices of Bangladesh was difficult and these were the main challenges of the study. The study is mostly based on literature, although the cyber-security and its reality in Bangladesh context-related issues is a less studied and thus limited literature is available regarding this topic. The present study attempts to shed light upon the threat posed by cyber-crimes in the context of the global village with an emphasis on the perspective of Bangladesh.

Keywords: Bangladesh; Cyber-crimes; Cyber-security; the ICT Act 2006; the Digital Security Act, 2018.

I. INTRODUCTION

The era of globalization is characterized by the rapid proliferation of information technology and communication. Secure cyberspace is the era of globalization and is a crucial element in maintaining national security. This plays an important role in achieving a country's economic stability and effective security [1]. Cyberspace is the world of computer networks (and the users behind them) where information is stored, exchanged and revealed [2]. With the rapid and dramatic growth of information and communication technology (ICT), cyber-crime has become a major security issue in the international arena. Both individual cybercriminals and state-sponsored cyber-attacks pose threats to states protecting their confidential data. Apart from having a profound impact on the economic progress and defence systems, these threats escalate diplomatic tensions leading to anarchy in the world order. Global peace, stability, and development might be affected by the abuse of information communication technology. Bangladesh with its less sophisticated cyber-surveillance system and cybersecurity tools may easily become a safe haven for cybercriminals committing phishing, hacking and stealing personal data. Digital services extended to people by the government and non-government sectors and personal and organizational data are targeted by criminals. Proper security measures are not often ensured while providing services through digital platforms. In addition, the Information Communication Technology Act, 2006 [3] might do little to secure cyberspace. This study endeavours to explore the major challenges for Bangladesh with its disarrayed cybersecurity and countermeasures in the context of the globalized world. In this respect, the study re-examined the efficacy of the existing information and telecommunication laws and proffers restitutive measures to ensure cybersecurity in Bangladesh. The study concludes with the utterance that the time is ripe for Bangladesh to enhance its cybersecurity and secure its cyberspace.

II. CYBER SECURITY IN THE GLOBLA VILLAGE

As the Internet connects virtually every human being living on the planet, a new coinage terming the global citizens as netizens. Cyber threats are no longer being seen as national security concerns, they are indeed global phenomena. Cybercrimes pose harm not only to individuals or specific target groups even to the states. Cybercriminals tend to exploit any potential loopholes at networks, systems, data, and operators to garner money. According to B. Williams, there are four Cybercrimes groups. First of all, cyber-criminals just after the money. Such an example came in April 2013 when the U.S. stock market suffered a $130 billion in minutes only because of a hacked Twitter news stream propagating a false story of an explosion at the White House [4]. Second, the competing organizations pursuing sensitive knowledge or intellectual property that could exploit them over others. In both the civil and security industries, this is worrying. A Russian crime organization recently cumulated the largest documented set of stolen internet data, consisting of 1.2 billion usernames and combinations of passwords, more than

500 million email addresses [5]. Thirdly, an insider de facto might pose a threat from within. Recent breaches of IT systems ranging from Iran's nuclear facilities to thousands of American diplomatic cables have underscored the importance of ensuring cyber-security in the Information Age. Cybercrimes because of their transnational nature and anonymity of the criminals are more exacerbating and their potential damage is disproportionate.

While a striking issue in its very own right, cyber-crime forecasts the inescapable clashes that will emerge from the close contact facilitated by the Internet between diverse cultural practices. The emergence of the Information Age has created an unparalleled network between people all over the world and also established connectivity at organizational scales. Intra-organizational and governmental communications have never been so rapid, cheap, and specific as the internet has taken the whole process of connectivity to an unprecedented dimension. Even information transmission to non-networked is also facilitated by common software platforms. Such connectivity, while helpful to all, comes at a potential cost. Globally governments and associations are while encountering umpteen cybersecurity occurrences, focusing on the management of cybersecurity threats and dealing with their fallout. For some associations, the most common cybersecurity threat is the danger of classified data being gotten to and possibly abused by an outside or potentially antagonistic party i.e. data breaches. One of the key difficulties in reacting to data breaches is that information, ruptured from one or more jurisdictions, can be passed instantly to other jurisdictions. The transboundary nature of occurrences can make investigating a data breach, distinguishing our alternatives for managing the breach, a mind-boggling and overwhelming procedure. This is particularly so on the grounds that speed is quite often a basic factor in exacting a compelling response. In the Asia Pacific region, there has been a rush of new digital security enactment in recent years, Governments establishing bodies to regulate or monitor digital security, and governments and controllers regularly issue guidelines/reports on this. For example, Indonesia and Singapore both launched cyber agencies in 2015, Japan approved the Cyber Security Basic Act, and a report on cyber resilience was issued by the Australian Securities and Investments Commission. Laws or guidelines on these matters are being formulated out of the blue for different nations in the Asia Pacific. Also countries, for instance, the United States, where the Justice Department released in April 2015 its "Best Practices for Victim Response and Reporting of Cyber Incidents", are adding to already existing frameworks of cybersecurity guidelines. Despite the intensive and exhaustive administrative action, there is, sadly, no combined approach to cybersecurity regulation or potential legal recourse with regards to data breaches in the Asia Pacific. Subject to change under varying jurisdictions, data breaches may include Responsibilities under data protection laws, employment/labour laws, equal rights and obligations, equity rules, corporate governance, fiduciary duties, and business or sector-specific legislation, in addition to cybersecurity laws. When data is believed to have been moved out of a jurisdiction, in some jurisdictions, state laws on national secrets can come into force. Similarly, local knowledge of responsibilities in each nation and how each applicable regulator or court works by and by is crucial for reacting to an episode of the data breach and knowing the legal remedies could be accessible and which would be better. Utilizing this learning, it can help the clients to examine data ruptures, to distinguish obligations, to devise plans to limit the further revelation of the data and moderation of impact or harm, and to recognize, where accessible, lawful solutions for recouping the information or loss related with the information rupture. Many of the Government's websites use international servers and foreign vendors. As a result, these are always in a vulnerable position and at risk of being sabotaged by the system's insiders [6]. Potentially the fourth strategy is the biggest threat to our national security. This relates to a state-sponsored cyberattack aimed at undermining a national security framework such as critical infrastructure or important national economic components to some degree in order to achieve strategic advantages over that specific country [7]. In this context, the instance of China can be cited. Some of the powerful countries in the world such as the U.S., U.K., France, Germany and India always consider China as a potential threat to cybersecurity and charged the country in connection with espionage for gaining strategic advantages. In 2007, it is confirmed that China launched a series of network-based cyberattacks on the above-mentioned countries. In addition, these countries do have greater military ambitions to boost the capacity of the country to engage in information or cyber warfare, if necessary in the near future [7].

III. CYBER VIOLANCE AGAINST WOMEN IN BANGLADESH

In Bangladesh, women are lopsidedly subjected to violence and harassment; cyberbullying to pornography are mentionable phenomena that are facilitated by the internet and other electronic devices. While the extension of Information and Communication Technology (ICT) and burgeoning Internet infiltration are considered as positive markers of development in the country, yet their association with certain existing socio physiological settings and insufficient legal protections have paved the way for extensive cyber brutalities against women. By and large, the type of this glaring infringement of human rights ranges from cyberstalking, vengeance pornography, cyberbullying, and trolling. Women are the primary targets of hostile and frequently forceful lewd gestures and disparaging messages on the internet from unidentified and counterfeit sources. Doctored nude pictures of women alongside spam, sex-act recordings, rape threats, and obscene proposition have turned into the new standard of social media. Mobile telephony has taken internet penetration by a storm with the number of active internet connections in Bangladesh hit 90.5 million in August 2018, of them, 80.47 million are connected with mobile internet [5]. The ever-increasing internet penetration and mobile phone devices have seen an upsurge of Facebook use. Of the 29 million registered Facebook users, 86% use mobile phones to access the social media networking site. Women population constitute 1% of cell phone and internet subscribers. Young women in Bangladesh are more likely to be victims of sexualized and abusive online violence in nature. Though legal framework and organizational protection is feeble, a sizeable number of women lodge formal complaints in connection with badgering, abuse, and violence emanating from cyberspace. Cybercrime has been reported by 73 percent of women internet users [18]. The Cyber-Help Desk of the government's Information and Communication Technology Division has received more

than 17,000 complaints as of December 2017, 70% of complainants being women. Exposure to pornographic content among the youths, whether intentional or unintentional, aggravates the other associated risks, for example, picture-based maltreatment of users where women are exceedingly victimized. In the digital world, around 78% cases of doctored photos containing pornographic contents, women are found to be the victims. It can be noted that nearly 77% of teenagers in the country regularly watch pornography. In June 2019, the Bangladesh National Women Lawyers' Association reported that badgering remained an issue and inadequate preventive and counteracting laws caused some young women to drop out of their classes or works because of trauma and stigma. The establishment of complaint committees and the installation of complaint boxes at educational institutions and workplaces mandated by the directive of the court have rarely been implemented [16]. Very often social media accounts are hacked with malicious intent. The criminals usually upload manufactured indecent photos of the victims, send provocative messages to the victims' contacts (i.e. Facebook friends) in order to disparage and humiliate them. Some of the key motives of these perpetrators include smearing the victims, taking revenge, coercing them to establish physical relationships, pressing for hush money, physically torment the victims, and so on. A pattern is seen while reviewing the lawsuits, investigation, and media reports of cyber violence against women in Bangladesh. Most commonly the perpetrators establish consensual physical contact with the victims earning their trust. They film the intimate moments with hidden cameras installed in the scenes, it is obvious if the pattern of these heinous crimes is observed closely. Unfortunately, it doesn't stop here, the criminals then go on to blackmail the victims and coerce them to gain their ill motives. Those clips are used later in order to force the victims to submit themselves to the will of the criminals demanding continuation physical relationships and hush money. Meanwhile, criminals often record the nefarious acts of rapes and film the incidents. Those video recordings are used later by the perpetrators to silence the victims to abuse them furthermore. Those recordings are most commonly released on the internet despite submissions of the victims making them traumatized and stigmatized in society. There are reports of deaths by suicide as the victims feel utterly helpless and do not find any headway. Another pattern is also noticed where vindictive ex-husbands and lovers post intimate videos or photographs on the internet to satisfy their grudges. As young women are less experienced to the internet they are most vulnerable to falling prey to the traps of cybercriminals.

A. Effects of cyber violence

The effects of cyber violence against women in a somewhat conservative society like Bangladesh is pervasive. The families of the victims are also greatly affected by such incidents. The series of events that follow are a double blow equally for the victims and their families often leaving them ostracized. People tend to believe whatever stuff they come across in social media. Such an indiscriminate belief system is the result of hollow public psychology stemming from a lack of awareness, ignorance, and education. Consequently, when a purportedly released photo of a girl surfaces on the internet mixed up with a raunchy gossip, general internet users bother little to verify whether the photo is real or fabricated. Merrily they go on to ogle at the contents and make those viral. This tendency to spread sex-related gossip amplifies the victims' sufferings manifolds. Not to mention the misery of the victim's family members who face social exclusion, humiliation, and public resentment [10]. The consequences of these cyber violence are disastrous at individual levels leading to severe depression, a sense of guilt, paranoia, and fear of harm to self and family members. Victim's career, education, and social life are jeopardized by these issues with some of them taking the path of drug addiction some choosing to end their lives. Very few of the victims recover from the trauma in a handful of exceptional cases. Bangladesh National Women Lawyers' Association tallied 65 reported suicide attempts by female victims subjected to such violence from 2010 to 2014. According to the findings of the association, on average there are 11 cases of suicide attempts by women due to cyber violence. Whereas the number of such cases was 8 in 2008, the data reveals an upward trend. However, the official statistics are nascent in comparison to the actual number of such incidents. The number of unreported cases far outweighs the reported ones [4].

IV. CHALLENGES OF BANGLADESH

The major concern for Bangladesh is that most of the software used in the country is pirated. In such a situation, it a big challenge for the country to protect its cyberspace in the poor infrastructural system. In Bangladesh, around 90% of software is pirated [3]. Right now, it has become a common practice and culture among the country people of using the pirated software, leading its cyberspace to the most vulnerable position in the cybersecurity domain. This is the major challenge the country is facing right now, but its consequences and impact cannot be ignored.

Apart from the concern, there are some other serious challenges for cybersecurity in Bangladesh that cannot be ignored any longer. According to Bangladesh Telecommunication Regulatory Commission (BTRC), in August 2018, the number of active internet connections in Bangladesh reached 9, 05 crore, which the matter of thanks to the introduction of around 18 lakh new connections to the network in one month. Among these, 8.47 crore connects to mobile internet, 57.33 lakh connects to fixed broadband internet while the rest use WiMAX. The total number of active Internet connections exceeded the seven-crore plateau in April 2017, the six crore mark in August 2016, five crore in August 2015 and four crores in September 2014, respectively. Such rapid growth of internet users in Bangladesh has put the country's financial sector under persistent cyber threat. In such a situation, it is an urgent need for strong in-built cybersecurity in Bangladesh. A small group of experts who work regularly on cyber-threat intelligence, data security, and encryption is also in desperate need.

To understand the challenges, first of all, we need to be conscious of the dimension of the cyber-crimes we are facing in our daily life. This may break it up into four groups. First, Cyber-crimes against people, such as: hacking or cracking, unlawful/unauthorized entry, illegal surveillance, data intrusion, e-mail spoofing, spamming, cheating and fraud, abuse and cyber-slaughter, slander, drug trafficking, virus transmission. And worms, infringements of intellectual property, abuse of machine and network resources, Internet time and information theft, forgery, denial of services, dissemination of pornographic materials etc. The second is property-related cybercrime, such as the robbery of credit card

money, intellectual property violations, Internet time theft, etc. The third one is organized crime. Examples of these crimes include unauthorized control/download over network resources and websites, posting of indecent/obscene content on web pages, virus assault, e-mail bombing, logic the bombing, trojan horse, data dodging, download blocking, theft of valuable belongings, terrorism against government organizations, vandalizing the infrastructure of the network etc. Fourth and last group of cyber-crimes are taking place against Bangladesh's society or social values. Such crimes include forgery, online gambling, prostitution, pornography (especially child pornography), financial crimes, and youth pollution by indecent exposure, web jacking, etc. [11].

In Bangladesh, pornography is one of the major concerns in terms of the country's social culture and moral values. We can now communicate with anyone anywhere in the world and share or exchange our cultural values, thanks to the rapid digital expansion and globalization. From the cultural perspective, many harmful elements of different country's culture easily can intrude to our own culture due to the diffusion of culture. Pornography is a very untoward element for the country's culture where adult education is not welcomed even. Bangladesh police are receiving a huge number of complaints of demanding ransom by threatening with secret nude video footage and photo shopped pornographic photos, according to the lawmen. Most of the victims are teenage girls. Besides, women and children are also being targeted by criminals. When any crime is conducted from abroad, then it would be considered as 'dual criminality'. That means the crime is considered in both countries. But there is a complexity to deal with the crime like pornography as such crimes [in the context of Bangladesh] may not be considered as crimes in many countries like the U.S. in every case. In such a situation, the victims in Bangladesh will have to face difficulties to deal with such crimes. On the other hand, transnational crimes like child pornography, which are considered as crimes in both countries and every country, can be dealing with international cooperation. Here an instance can be given of such an issue.

Several years back, Tipu Kibria, a well-known child litterateur in Bangladesh, was arrested by police red-handed for child pornography. He used street male kids in his home and lab to make pornographic videos and photo shooting for girls. He had already assaulted some 400-500 street kids at the time he was arrested by police for his filthy ambition. Throughout these illegal activities, he has two assistants to help him out, and police found 13 foreign buyer names from Tipu Kibria who regularly paid him for weekly supplies via foreign or online banking transactions. Bangladesh police also believe that there might also be several other manufacturers other than Tipu Kibria. We may therefore explicitly state that pornography is a major concern regarding cybersecurity in Bangladesh [1]. Cybersecurity threat, especially for the financial transaction including e-commerce and online banking is also a grave concern for Bangladesh. Besides, transnational crimes like drug smuggling, trafficking, terrorism etc are other big challenges to Bangladesh's cybersecurity. Due to lack of proper cybersecurity measures, Bangladesh is also facing a serious concern of cyber threat in the banking sector.

In February 2016, Hackers stole $101 million from Bangladesh's central bank account with the Federal Reserve Bank of New York using the SWIFT payment network for fake orders. Cyber heist is one of the world's greatest cyber-crimes. If Bangladesh fails to take proper measures and adopt strong security policies, the country's banking sector may become the further victim of such cyber heist in the coming days. Widespread use of credit cards and that electronic payment methods often risk a large number of private customer details, such as bank account name, bank account number, cell phone, e-mail ID etc. [3]. The law enforcement agencies are often receiving complaints or cases of direct or indirect cyber threats to financial transactions through online banking. On February 12, 2016, Eastern Bank, a private bank in Bangladesh 21 Suspicious card transactions found. A fraudster with a fake EBL card used one of United Commercial Bank Limited's ATM Booths, which set off the alarm in UCBL's network, causing the crime ring to unravel. On February 25, Dhaka Metropolitan Police said that the investigation of the ATM Card scam case has brought up names of various hotel travel agencies and some bank officials. The lawyers also detained a German citizen in connection with ATM fraud, and three official City Bank, a local private bank. Piotr was wanted in 3-4 countries on fraud charges, and according to police, we would be seeking information from those countries through the Interpol.

Some Bangladesh-based foreigners have allegedly been involved in the skimming scam that robbed money from ATMs in signs of emerging financial crimes that terrified both banks and customers. In February 2016, Bangladesh Bank, three other commercial banks and lawyers analysed video footage of four ATM Booths, which were skimmed off at least Taka 25 lakh. The spokesperson for the central bank said they mainly find the involvement of at least two foreign nationals in the crimes. There are similar concerns in different private banks like — Eastern Bank Limited, United Commercial Bank Limited and City Bank — struck by ATM frauds (The Daily Star, February 16, 2016). All the banks both private and government commercial banks are taking security measures to curb illegal transactions. But due to the lack of proper and adequate security measures and technological support and responsibility of the authorities concerned, the country's troubled banking sector is still struggling to face the cybersecurity challenges. Besides, many people in Bangladesh are being victimized by phishing or fraudulent attempts to get confidential evidence like usernames, passwords, and credit card details through e-mails or attractive advertisements. In these cases, victims typically lose $100-500 per case and refuse to go to the police to complain, which makes the case in Bangladesh more difficult to deal with [1].

Hacking or unauthorized intrusion into a computer system without the owner or user's permission is also a concern for the cybersecurity in Bangladesh [11]. Hackers most of the time targeted the financial websites of both the government and prominent privates organizations. Lack of adequate cybersecurity know-how, Bangladesh is in a more difficult position to tackle cyber-piracy by a weak cyberinfrastructure network such as reliance on international server system providers, etc. [1]. Data-stealing is another concern in Bangladesh. The leak of Bangladesh War Crime Tribunal's verdict (partially) in 2014 is an example of the data-stealing. The data of the tribunal leaked through Skype's voice recording. It was a major backlash for the Bangladesh government and exposed the vulnerability of the Bangladesh cybersecurity arena [1]. Besides, cybersecurity of social media platforms especially Facebook, Twitter, and Linkedin are in grave threat in

Bangladesh. Though Bangladesh police, Bangladesh Telecommunicate Regulatory Commission have strengthened monitoring and established separate monitoring teams recently, such hacking of social media accounts are happening frequently till February 2019. Hackers are targeting mostly prominent personalities, celebrities and females and taking money from the victims threatening of tarnishing their social image.

V. EXISTING ACTS AND THEIR LIMITATIONS

Right now, there is no debate about the level of cybersecurity risk in Bangladesh, but the major concern is whether the country would be able to address the risk properly and timely. It is sorry to say that the concerned authorities are still reluctant to take full-scale measures to combat the risk, thanks to the lack of understanding in different concerned stakeholders. To combat the cyber-crime, the Bangladesh government has formulated a few laws including Information and Communication Technology (ICT) Act, 2006 [8] and Digital Security Act, 2018. But literally, these laws are seen largely to be used in curbing the freedom of speech and expression. Some contradictory articles and sections of the laws are being used by the government and law enforcement agencies to gag the news media and social media. Bangladesh government passed the ICT Act on October 8, 2006. Seven years after its formulation, the parliament of the country amended the act keeping some controversial provisions on 6th October 2013. However, a cyber-crime victim can sue someone under the law for cyber-crime regardless of his or her place and location in the world. Victims may at least use this ICT Act as a starting point, but after that, they certainly need strong cooperation to make progress from first, regional law enforcers in Bangladesh with expertise in cybersecurity such as CID (Criminal Investigation Department) and from foreign law enforcers such as Interpol [1]. Human rights advocates, representatives of civil society, and media critics urgently demand that section 57 of the Information and Communication Technology Act be repealed as such clause of law provides room for widespread misuse. The maximum penalty for offenses under the section before its amendment was 10 years imprisonment and a fine of Taka 1 crore. However, law enforcers had to take permission from the appropriate authorities to file a case however arrest any person under the rule. After the 2013 amendment, the maximum jail term was raised to 14 years. In addition, legislators were granted the right to detain someone without a warrant. A rough translation of section 57(1) says, “If any person deliberately publishes or transmits or causes to be published or transmitted in the website or in any other electronic form any material which is false and obscene and if anyone sees, hears or reads it having regard to all relevant circumstances, its effect is such as to influence the reader to become dishonest or corrupt, or causes to deteriorate or creates the 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 will be regarded as an offense.” Despite the reforms with a few significant changes, the 2006 key Act remains unchanged with all its inconsistencies and imposes unnecessarily harsh punishments [2]. However, the 2013 ICT Act (amended) has become the Bangladesh government's tool for violating fundamental human rights, such as freedom of opinion and expression. The act includes a range of ambiguous imprecise and overboard clauses [9] that could help to further instigate rather than contain cyber-criminal activities. According to the ICJ, section 57 of the original ICT Act is 'incompatible with the obligations of Bangladesh under Article 19 of the ICCPR: the offenses imposed are ambiguous and excessive; the limitations on freedom of speech and opinion go beyond what is allowed under Article 19 (3) of the ICCPR' [9]. J. Barua said, “Section 57 is not specific and covers a wide area of offenses, there will be little chance to get an acquittal from any charge” [2]. After reviewing the ICT Act 2006 with its amendments, we may conclude that there should be legislation to cover cyber space-related crimes, but the current act is ambiguous and needs to be structured on a permanent basis as a modernist legal structure, not only based on the ad hoc system.

From the very beginning, rights activists and journalists were critical of Section 57, and the debate on the provision and demand for its abolition escalated after the arrest of journalist Probir Sikdar in 2015. In addition, under section 57 of the Information and Communication Technology Act, at least 21 journalists were sued in four months to July 2017 in the face of the growing demand for the abolition of the provision that is widely open to misuse (The Daily Star, 7 July, 2017). Amid widespread criticism of the ICT Act, on May 2, 2017, Bangladesh Law Minister Anisul Huq said that section 57 would be withdrawn and a new "Information Technology Act in the pipeline" will be implemented. On 19 September 2018, Bangladesh's Parliament passed the 2018 Digital Security Act with a tough clause authorizing police officers to search or arrest someone without warrant Rights activists and journalists expressed concern that the act goes against the constitutional spirit and would restrict freedom of speech, freedom of expression, freedom of thought and hinder independent journalism. Section 43 of the new law specifies that when a police officer believes that an offense has been committed or is being committed at a given location, where there is the risk of committing offenses if evidence is lost, the official can search the location or any person there. *Sampadak Parishad* (The Editors' Council), a daily editorial forum in Bangladesh expressed surprise, frustration, and shock in a statement on 16 September last year, it said the sections 8, 21, 25, 28, 29, 31, 32, and 43 of the act poses serious threats to freedom of expression and media operation. Section 3 of the Digital Protection Act incorporates a clause of the Access to Information Act 2009 which will extend to information-related matters. Where a person commits any crime or assists others in committing crimes under the Official Secrets Act, 1923, as provided for in section 32 of the law, through a computer, digital device, computer network, wireless network or any other electronic medium, he or she may face a maximum of 14 years in prison 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 themselves to, and our brave martyrs to sacrifice their lives in, the national liberation struggle.” Under section 29 of the law , a person can face up to three years' imprisonment or a fine of Tk 5 lakh or both if he or she commits the offenses provided for in section 499 of the Penal Code via a website or electronically. Section 31 of the Act states that a person may face up to seven years in prison or Taka 5 lakh in fine or both if he or she is found to have intentionally published or broadcast something on a website or in electronic form that may spread hate

and build enmity between different groups and communities, and may cause deterioration in law and order (The Daily Star, 20 September 2018).

VI. POLICY OPINIONS

We can provide several remedial policy options in the above scenario regarding cybersecurity, cyberspace safety, and reducing cyber-crime rates in Bangladesh. We suggest policy options for the government in Bangladesh, but it also includes the individual security domain. . These options could be as such:

A. Reform of legal structure

We resound with the ICJ's legal recommendations about the ICT Act 2006 and its amendments to both the Bangladesh Parliament and the Government of Bangladesh. The ICJ refers to the Bangladesh Parliament for all reasons, 'Repeal the Information and Communication Technology Act 2006 [8], as amended in 2013, as amended in 2013, or amend the ICT Act to bring it into line with international laws and standards including the legal obligations of Bangladesh under the ICCPR. At a minimum, this will require it (1) to amend section 57 of the ICT Act in order to ensure that any envisaged limitations on freedom of expression and opinion are in accordance with international law and standards; (2) to amend section 57 of the ICT Act to ensure that forbidden speech is clearly defined; (3) Amend the ICT Act to ensure that any restriction on freedom of speech and information, including any penalty provided for, is necessary for a valid purpose and proportionate to the harm caused by that speech " [9]. In this regard the ICJ also proposed policy alternatives to the government of Bangladesh. Such policy options are: (i) 'Take action to ensure that the provisions of the ICT Act are not used to infringe the right to freedom of speech, including restricting the legitimate exercise of public opinion on matters which may include criticism of the Government; (ii) drop charges against bloggers for the legitimate exercise of their freedom of expression; (iii) Guide government agencies to refrain from filing unfairly limiting the freedom of speech in politically motivated cases and to pursue penalties disproportionate to the severity of the alleged offence; [9].

B. Maintaining rules of cyber security

In 2011, in his article 'Ten Rules of Cyber Security,' Eneken Tikk, the legal counsel at the NATO Cooperative Cyber Defense Center of Excellence, Tallinn, Estonia, provided a measured framework to preserve cyber security tenets considering national security issues as well as individual security concerns. Eneken Tikk's propositions are agreeable in many cases. He talked about 'the territorial rule' protecting cyber security as such, "Information infrastructure located within a state's the territory is subject to that state's territorial sovereignty" [15]. Tikk also spoke of 'the law of duty' where he proposed that the States behave responsibly to secure their own territories. He also spoke of the 'early warning statute' as such, "There is an obligation to notify potential victims about known, upcoming cyber-attacks" [15].

By examining Tikk's above cybersecurity rules, we can prescribe a solid national digitally insightful agency for Bangladesh to battle present and forthcoming potential cyber threats from anyplace of the world as they say counteractive action is superior to fix. Secondly, in Tikk's opinion, a state should adopt 'the data protection rule' protecting its vital national data. In his words, "Information infrastructure monitoring data are perceived as personal unless provided for otherwise." In this context, another rule of Tikk can be cited here, 'the duty to care rule'. He is suggesting everyone take a minimum level of responsibility to secure any kind of information infrastructure [15]. By resounding his idea, we can propose that the Bangladesh Government exploit her own resources, skills, and implement trend-setting innovation to secure the internet and national interests. Imparting training to our cyber experts, building up own server frameworks and systems utilizing our own assets and labor, investing a sizeable amount of time to build up our cyber safety net, recruiting potential national programmers and so on can be beneficial to Bangladesh over the long haul as opposed to depending on foreign specialists. 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" [15]. 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" [15]. We need solid worldwide participation to fight any sort of cyber security risk as to the majority of the cases, these threats have been included with transnational criminal exercises where the affected individuals might be victimized in one country and culprits may flee by taking advantages of international border boundaries. Bangladesh Government and Bangladesh Police have joined hands with international law enforcing agencies, for example, Interpol in such manner yet Bangladesh needs more collaboration particularly from the tech giants, for example, Microsoft, Google, Facebook, Yahoo and others. In conclusion, Tikk's other two rules--' self-defense and the access to information rule--can be referred. 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" [15]. As we quote him, we recommend that the Bangladesh government takes preemptive and precautionary measures to ensure cybersecurity at the individual and national levels.

C. Individual awareness

The consequences and reality of globalization is undeniable. Awareness of personal data protection and safety must be developed at individual level apart from government, initiatives to create secure cyberspace. Professionals irrespective of their hierarchy and varying organizational structures must gain a minimum level of expertise in handling cyber technologies and building awareness on cybersecurity threats does not seem to have any alternative. Only proper education and awareness can rescue Bangladesh from falling into the deep a pitfall of cybersecurity threats [1]. Basic precautionary measures should be exercised while using the internet. Here are some preemptive measures that can be taken:

(i) Keep trustworthy and restricted personal details (ii) Keep your privacy settings on (iii) Secure browsing (iv) Make sure your internet connection is safe (v) Be careful what you access (vi) Use good passwords (vii) Make online transactions from protected sites (viii) Be careful what you post (ix) Keep your antivirus software up to date. If we think if we have been a victim to cybercrime, we should go to our local police station, in some scenarios, contacts the FBI and Federal Trade Commission. Even if the crimes seem trivial, it is

important to report such incidents. Our promptness may prevent the recurrence of such crimes. If we suspect identity theft, contact the financial institutions and companies where the fraudulence occurred.

VII. CONCLUSION

Taken everything into account, the issue of cybercrimes is emerging as a global phenomenon which poses potential threats to the national security of any country and Bangladesh is no exception to that rather the issue of cybercrimes is more worrying for the country in the context of globalization. Because of the absence of advanced cybersecurity tools and people's ignorance in handling tech gadgets coupled with lack of awareness in cyber security threats might have disastrous impacts on the country. In addition, the country's laws seem inadequate to safeguard the cyberspace of the country. International collaboration, enhancing technical know-how, gaining expertise and campaigning on people's preparedness on how to deal with cybersecurity threats are some of the remedial aspects the country may take into consideration to combat ever-looming cybersecurity threats. The sharp increase in cyber-crimes in Bangladesh and all over the world validates the propositions that the issue of cyber-crimes is undeniable though some argue may that the cyber threats may not be the possible near-future scenario for Bangladesh. Finally, on a note of conclusion, it can be stated that the time is ripe for Bangladesh to take preemptive and counteracting measures to thwart the threats posed by cybercriminals. In this regard, Bangladesh government and the general people can mull over the suggestions provided in this paper.

ACKNOWLEDGEMENT

I Dr. Kudrat-E-Khuda (Babu), would like to express my gratitude to all those who gave me the possibility to complete this paper. I want to thank the Daffodil International University, Bangladesh for giving me permission to commence this paper in the first instance, to do the necessary research work. I am deeply indebted to my younger brother Mr. Sujon Ali, University of Rajshahi, Bangladesh whose helps, stimulating suggestions and encouragement helped me in all the time of research for and writing of this paper.

REFERENCES

[1]. Alam, S. (2019). Cyber Crime: a new challenge for law enforcers. *City University Journal, 2*(1), 75-84.

[2]. Barua, J. (2015). Amendment Information Technology and Communication Act. *The Daily Star,* p. 5. Retrieved from http://www.thedailystar.net/supplements/amended-information-technology-and-communication-act-4688

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

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

[5]. BTRC (2018). Internet Subscribers. Bangladesh Telecommunication Regulatory Commission. Retrieved from http://www.btrc.gov.bd/content/internet-subscribers-bangladesh-april-2018.

[6]. Editorial (August 20, 2013): Draft ICT (Amendment) Ordinance-2013: a black law further Blackened. *The Daily Star*, p.8. Retrieve from http://archive.thedailystar.net/beta2/news/draft-ict-amendment-ordinance-2013

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

[8].The Information and Communication Technology Act (2006). The ICT Act, 2006. Retrieved from http://www.prp.org.bd/downloads/ICTAct2006English.pdf.

[9]. International Commission of Jurists (2013).Briefing Paper on the Amendments to the Bangladesh Information Communication Technology Act. Retrieved from http://icj.wpengine.netdna-cdn.com/wp-content/uploads/2013/11/ICT-Brief-Final-Draft-20-November-2013.pdf.

[10]. Karaman, S. (2017). 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. Retrieved from http://blogs.lse.ac.uk/wps/2017/11/29/women-support-each-other-in-the-fa.

[11]. Maruf, A. M., Islam, M. R. and Ahamed, B. (2014). Emerging Cyber Threats in Bangladesh: in quest of effective legal remedies. *The Northern University Journal of Law, 1*(10), 112-124. Retrieved from https://www.banglajol.info/index.php/NUJL/article/view/18529.

[12]. Elahi, S. M. (2014). Porn Addicted Teenagers of Bangladesh. Dhaka: Manusher Jonno Foundation.

[13]. Perlroth, N. and Gellesaug, D. (2014). Russian Hackers Amass Over a Billion Internet Passwords. Retrieved from http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen internet.

[14]. Singer, P. W. and Freidman, A. (2014). Cybersecurity and Cyberwar: what everyone needs to Know. Oxford: Oxford University Press.

[15]. Tikk, E. (2011). Ten Rules for Cyber Security-Survival: Global Politics and Strategy. London: Routledge & CRC Press.

[16]. USSD (2017). Country Report on Human Rights Practices for 2016. Washington DC: US Department of State. Retrieved from https://www.state.gov/j/drl/rls/hrrpt/2016humanrightsreport/index.htm?ye.

[17]. Williams, B. (2014). Cyberspace: what is it, where is it and who cares? Retrieved from http://www.armedforcesjournal.com/cyberspace-what-is-it-where-is-it-and-who-cares/.

[18]. Zaman, S., Gansheimer, L., Rolim, S. B. and Mridha, T. (2017). Legal Action on Cyber Violence against Women. Dhaka: Bangladesh Legal Aid Services Trust (BLAST).

How to cite this article Kudrat-E-Khuda (Babu) (2020). Cyber Security and its Reality in Bangladesh: An Analysis of Existing Legal Frameworks. *International Journal on Emerging Technologies, 11*(5): 425–431.